



CC-DRIVER

Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour.

D4.2 – Cybercrime vulnerability self-assessment questionnaire

[WP4 – Tools and training materials for LEAs, cybercrime vulnerability self-assessment]

Lead contributor	Lavinia Dincă, SIMAVI
	lavinia.dinca@simavi.ro
Other contributors	Otilia Bularca, SIMAVI
	Afonso César, PJ
	Meltini Christodoulaki, FORTH
	Christine Burkhardt, UNIL
	Eirini Papadopoulou, KEMEA
	Pavlos Kolovos, HP
	Julia Davidson, UEL
	Kirsty Philips, UEL
	Mary Aiken, UEL



Sven-Eric Fikenscher, BayHfoeD

Ruby Farr, UEL

Due date

31.12.2021

Delivery date

31.12.2021

Type

Report

Dissemination level

PU = Public

Keywords

Cybercrime vulnerability self-assessment questionnaire, technical requirements
--

Abstract

This document details the functionalities of the vulnerability Self-Assessment Questionnaire (SAQ) application. SAQ will allow the design of questionnaires using the graphical interface. SAQ application is independent of the questionnaires created, so users of the application can use it to create various questionnaires to test their security readiness in various security topics.

As part of the project a questionnaire suitable for SMEs and CSOs will be created in order to help them with cybersecurity defences, organisational measures, cost-benefit considerations, awareness of fundamental rights such as the rights to privacy, protection of personal data and the free movement of persons. The questionnaire created in SAQ application will be sent to SMEs and CSOs to be filled in anonymously. The system will generate complex anonymous statistics.

Revision Procedure

Version	Date	Description	Reason for Change	Author(s)
V0.1	29.01.2021	First Draft	Document outline, defined user management flows	Lavinia Dinca
V0.2	12.02.2021	New chapter	Questionnaire design and management	Lavinia Dinca
V0.3	22.03.2021	New chapter	Questionnaire response and security assessment	Lavinia Dinca
V0.4	20.04.2021	New chapter	Campaign, update chapter questionnaire design	Lavinia Dinca
V0.5	15.05.2021	New chapter	New chapter: campaign statistics	Lavinia Dinca
V0.6	30.06.2021	Updates	Update flow chapter and modify terminology for consistency, updates on FR and NFR lists, abstract, and introduction	Lavinia Dinca
V0.7	30.09.2021	New chapter	Questionnaire content and dissemination	Lavinia Dinca
V0.8	29.10.2021	Updates	Questionnaire content proposal – 40 initial questions	Lavinia Dinca
V0.9	11.11.2021	Updates	Full document review- ready for partner review	Lavinia Dinca
V0.91	10.12.2021	Updates	Implement partner review comments	Lavinia Dinca
V1.0	17.12.2021	Final Version	Final document review – currently awaiting approval by the EC, watermarked as draft until approval.	Lavinia Dinca

Contents

<i>Abstract</i>	2
<i>Executive summary</i>	6
<i>Disclaimer</i>	6
<i>Copyright notice</i>	6
<i>List of figures</i>	7
<i>List of tables</i>	7
<i>List of equations</i>	8
<i>List of acronyms/abbreviations</i>	9
<i>Glossary of terms</i>	10
1. Introduction	11
1.1 Background	11
1.2 Objectives	11
1.3 Structure of the report	12
1.4 Scope and limitations	12
2. Methodology	13
2.1. Functional requirements design methodology	13
2.2. Non-Functional requirements design methodology	14
2.2.1. Security overview	16
2.3. Personal data collected by the application	18
3. Functional Requirements list	19
4. Non-Functional requirements list	19
5. Application Flows	20
5.1. Account management	22
5.1.1. User creation	22
5.1.2. Validation	23
5.1.3. User authentication	23
5.1.4. User administration	25

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

5.1.5.	User profile	26
5.2.	<i>Questionnaire design and management</i>	27
5.2.1.	Questionnaire design list	27
5.2.2.	New questionnaire	28
5.2.3.	Admin questionnaire menu	33
5.3.	<i>Campaign</i>	34
5.3.1.	Campaign list	34
5.3.2.	Campaign creation	35
5.3.3.	Campaign viewing	36
5.4.	<i>Campaign response</i>	38
5.4.1.	Response start	38
5.4.2.	Campaign questionnaire fill-in	40
5.4.3.	Individual security assessment	41
5.5.	<i>Campaign statistics</i>	43
5.5.1.	Design screen with formulas	44
5.5.2.	Design screen with data	50
5.5.3.	View individual responses (and assessments)	53
5.5.4.	Download all data	54
6.	<i>Questionnaire design and content</i>	54
6.1.	<i>Introduction</i>	54
6.2.	<i>Industry benchmarking: common attack vectors</i>	55
6.3.	<i>Industry benchmarking: best practices</i>	61
7.	<i>Conclusion</i>	70
	<i>Annex 1 – Correspondence matrix</i>	72
	<i>Annex 2 – Vulnerability self-assessment questionnaire</i>	73
	<i>References</i>	81

Executive summary

This deliverable (D4.2) is part of Work Package 4 (WP4) that focuses on the creation of a vulnerability self-assessment questionnaire that will help SMEs and CSOs assess their vulnerability to cybercrime.

The scope of this deliverable is twofold: the first is to detail the application functionalities (the requirements specifications) which will be used to develop the SAQ application. The second is to create and define the vulnerability assessment questionnaire that will be sent to SMEs and CSOs.

Because this deliverable must incorporate results that will be delivered later than task 4.3, we'll develop the application that will allow the creation of the questionnaire independently of the questionnaire content. This way we can update the questionnaire content very easily.

Disclaimer

The information, documentation and figures available in this deliverable were written by the CC-DRIVER (Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour) project consortium under EC grant agreement 883543. The views expressed in this document should in no way be taken to reflect the views of the European Commission, nor can the European Commission be liable for any use made of the information contained herein.

The commercial use of any information contained in this document may require a licence from the proprietor of that information. Neither the CC-DRIVER consortium as a whole nor any partner in the CC-DRIVER consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, nor do they accept any liability for loss or damage suffered from using this information.

Copyright notice

© 2019 - 2022 CC-DRIVER Consortium

List of figures

Figure 1 TOGAF categories for non-functional requirements Source: https://dalbanger.wordpress.com/	15
Figure 2 CIA Triad Source: https://wizardcyber.com/	16
Figure 3 User creation	22
Figure 4 User validation	23
Figure 5 User Authentication	24
Figure 6 Password reset.....	25
Figure 7 User Management	25
Figure 8 User Modification by Admin.....	26
Figure 9 Password change.....	27
Figure 10 Questionnaire list	28
Figure 11 New questionnaire	29
Figure 12 Saved Questionnaire	29
Figure 13 Questionnaire navigation	30
Figure 14 Question creation	31
Figure 15 Publish questionnaire.....	33
Figure 16 Questionnaire management admin.....	34
Figure 17 Campaign list	34
Figure 18 New campaign	35
Figure 19 Campaign viewing	37
Figure 20 Campaign response closed state	38
Figure 21 Campaign response start	39
Figure 22 Campaign questionnaire fill-in	40
Figure 23 Questionnaire individual security assessment	41
Figure 24 Campaign statistics design screen with formulas	44
Figure 25 Campaign statistics design screen with data.....	52
Figure 26 Campaign statistics view responses	53

List of tables

Table 1 List of acronyms/abbreviations	9
Table 2 Glossary of terms	10
Table 3 FR specifications	13

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

Table 4 Functional requirements template 13

Table 5 Non-functional requirements template..... 15

Table 6 Personal data collected by SAQ application 18

Table 7 Functional requirements list..... 19

Table 8 Non-functional requirements list..... 20

Table 9 Application entities 21

Table 10 Dummy campaign information 50

Table 11 Dummy campaign response data 51

Table 12 Attack vectors raw data 58

Table 13 Deliverable D2.1- results synthetisation 59

Table 14 Vulnerability assessment test areas 64

Table 15 Classification of the questions 65

Table 16 Correspondence matrix 72

List of equations

Equation 1 Current questionnaire score 32

Equation 2 Questionnaire score calculation 42

Equation 3 Average score per round 45

Equation 4 Average score percentage per campaign 45

Equation 5 Max score per campaign 46

Equation 6 Max score percentage per campaign..... 46

Equation 7 Min score per campaign..... 46

Equation 8 Min score percentage per campaign 46

Equation 9 Pseudocode for number of responses over 70% per round..... 47

Equation 10 Percentage of responses over70 per campaign 47

Equation 11 Pseudocode for number of responses below 50% per campaign..... 48

Equation 12 Percentage of responses below50 per campaign (relative to number of responses)
..... 48

Equation 13 Pseudocode for all questions with score below 50% per campaign 49

List of acronyms/abbreviations

Abbreviation	Explanation
2FA	2 Factor Authentication
BEC	Business email compromise
CIA	Confidentiality Integrity Availability
CIS Controls	Critical Information Security Controls
CSO	Civil Society Organisation
DBIR	Data Breach Investigations Report
DDoS	Distributed Denial Of Service
EAC	Email Account Compromise
ERD	Entity Relationship Diagram
FR	Functional Requirement
HTTPS	HyperText Transfer Protocol Secure
MiTM	Man in The Middle
NFR	Non-Functional Requirement
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
SAQ	Vulnerability Self-Assessment Questionnaire
SANS	SysAdmin, Audit, Network, and Security
SME	Small Medium Enterprise
WP	Work Package

Table 1 List of acronyms/abbreviations

Glossary of terms

Term	Explanation
CIA	The CIA triad is the cornerstone of cyber security and represents: confidentiality, integrity, availability
FR	Core application functionality
HTTPS	Encrypted version of HTTP which allows to access web applications over the Internet in a secure way
NFR	Functionalities referring to how the system must work

Table 2 Glossary of terms

DRAFT

1. Introduction

1.1 Background

The CC-DRIVER project aims to examine the drivers behind cyber-criminality in the European Union (EU), emphasising the factors that lead young people to cybercrime, as well as cybercrime-as-a-service. Part of this project is the creation of a Vulnerability Self-Assessment questionnaire (SAQ) that can help Small and Medium Enterprises (SMEs) and Civil Society Organisations (CSOs) to protect themselves by embarking on cybersecurity defences, organisational measures, cost-benefit considerations, awareness of fundamental rights such as the rights to privacy, protection of personal data and the free movement of persons.

This deliverable D4.3, is a product of task 4.3 in WP4 which states:

“This task focuses on creating a self-assessment questionnaire so that SMEs, civil society organisations and other stakeholders can assess their vulnerability to cybercrime attacks. SIMAVI and the other partners will develop the online questionnaires taking into account the research findings from WP2 and the requirements from WP3. The user will be able to complete the questionnaire in an anonymous way. They will receive a score and afterwards guidelines on the countermeasures that they can undertake against the vulnerabilities.”

This document will describe the SAQ requirements specifications – the application functionalities.

1.2 Objectives

The purpose of this deliverable is to respond to task 4.3 from WP4 which has the following objective:

“The main goal of this WP is to integrate the findings of WP2 and WP3 in the development and validation of specific tools for LEAs and questionnaires for SMEs, CSOs and young people. At the same time, the tools will support the research work in WP3. WP4 has the following specific objectives:

*Produce a cybercrime vulnerability self-assessment questionnaire for SMEs and CSOs.
Design, develop, validate and pilot a set of tools assisting LEAs in fighting cybercrime.
Develop and test training materials for LEAs.”*

This deliverable explicitly covers the Objective 3 and R8 as defined in the Grant Agreement:

“Objective 3: *Create an online questionnaire that young people and organisations can use to assess their vulnerability to cybercrime. [...] We will also develop and demonstrate a self-assessment questionnaire on the CC-DRIVER website that SMEs, civil society organisations and others can use to check their vulnerability to cybercrime attacks. Stakeholders will be able to download the self-assessment questionnaire or complete it anonymously via the EU survey website.*

R.8: *The scoring of each user will derive from which of the five responses users tick to each question. CC-DRIVER will first develop a questionnaire suitable for SMEs and*

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

CSOs across Europe. The questionnaire will not be more than 10 pages and will be structured according to different types of questions - use of cybersecurity defences, organisational measures, cost-benefit considerations, awareness of fundamental rights such as the rights to privacy, protection of personal data and the free movement of persons. Completion of the questionnaire will generate a score, benchmarked against the aggregated scores of other stakeholders as well suggestions for countermeasures. Target audience: SMEs, CSOs, think-tanks. A self-assessment questionnaire on the CC-DRIVER website that SMEs, civil society organisations can use to check their vulnerability to cybercrime attacks.

***KPI:** Dissemination of the online cybercrime vulnerability self-assessment tool to national SME associations by M20 with 100 responses from SMEs and CSOs to the online self-assessment questionnaire before the end of the project.”*

The grant agreement states that the Vulnerability Self-Assessment Questionnaire (SAQ) will incorporate the knowledge from the partners and the results from other tasks in WP4. These other tasks will finish later in the project, whereas task 4.2 finishes at the end of 2021. To tackle this problem, we will divide the self-assessment questionnaire task into two parts:

- **Application (SAQ)** - we will create a SAQ application, that will allow users to design questionnaires, track, and see statistics in a graphical mode. The SAQ application is independent of the content of the questionnaire itself. This tool can be used to define any type of self-assessment questionnaires, not only related to security. Many companies, not only those involved in the project, can use this tool.
- **The content** – the questionnaire itself. The questionnaires will be defined in a graphical interface that can be used by a person with non-technical skills. We'll be able to easily incorporate results from later tasks just by changing/updating the questionnaire content.

The purpose of this deliverable is to detail the functional requirements for the SAQ application.

The functionalities detailed in this document will be used to develop the application.

1.3 Structure of the report

Following the foregoing brief introduction of Deliverable D4.2, the next section, Section 2 details the methodology used for requirements specifications. Section 3 provides a list of main functional requirements. Section 4 details the most important non-functional requirements. Section 5 describes the application flows and details functionalities. Section 6 details information about the questionnaire content and dissemination information. Section 7 concludes the document.

1.4 Scope and limitations

This document presents the flow of the application including design screens. The design screens are for presentation only they might be changed for clarity during development, but the application will contain the same information presented in this document.

2. Methodology

This chapter details methodology used in the requirements elicitation phase that will be used in the design of the SAQ application. The goal of this chapter is to explain the methods used for defining the functional requirements and the non-functional requirements and the difference between them.

2.1. Functional requirements design methodology

The Functional Requirements (FRs) are the main subject matter of the proposed SAQ application for CC-DRIVER and describe precisely what and in which way the application should function. The functional requirements describe the behaviour of a software system as it relates to the system's functionality (i.e., what a software system should do).

The functional requirements are related to the use of the software system in the real-world and to the end-user needs and expectations.

Our approach presumes that functional requirements are associated to each SAQ functionality, and they will be described as detailed in Table 3.

Functional Requirement ID	Requirement description
Unique identifier of the functional requirement like FR1	Description of FR following the proposed syntax - IEEE 29148 - 2018 - ISO/IEC/IEEE International Standard - Systems and software engineering - Life cycle processes - Requirements engineering

Table 3 FR specifications

The MoSCoW (Must Have; Should Have; Could Have; Won't Have) method was considered as appropriate for prioritising the development of requirements. A specific column for prioritisation in development was then added to the initial requirements table. The final structure for presenting the functional requirements is shown in Table 4 below:

FR ID	Description	MoSCoW	Chapter
FR1	The system should provide a basic questionnaire and framework for security culture assessment	M	Chapter number

Table 4 Functional requirements template

A significant part of defining functional requirements is represented by standardisation and more particularly by matching method and concepts with the rules and principles of standardisation. Using the appropriate standards for the functional requirements definition /

formalisation, it is provided a basis for applying a uniform structure and a common terminology.

A functional requirement is defined pursuant to guidelines of IEEE 29148 - 2018 - ISO/IEC/IEEE International Standard - Systems and software engineering - Life cycle processes - Requirements engineering [IEE18].

The IEEE Standard 1233-1998, IEEE Guide for Developing System Requirements Specifications [IEE98], defines a well-formed requirement as a statement that “can be verified, has to be met or possessed by a system to solve a stakeholder problem or to achieve a stakeholder objective, is qualified by measurable conditions and bounded by constraints and defines the performance of the system when used by a specific stakeholder or the corresponding capability of the system, but not a capability of the user, operator, or other stakeholder.”

The formalisation of a functional requirement supposes the compliance with a specific syntax, such as:

I. [Condition] [Subject] [Action] [Object] [Constraint]

Example: "When signal X is received [Condition], the system [Subject] shall set [Action] the signal received bit [Object] within 2 seconds [Constraint]"

II. [Condition] [Subject] [Action]

Example: "If the software platform is operational [Condition], the system [Subject] shall be capable of running what-if scenarios by means of a simulation component [Action]."

By applying MoSCoW method, the functional requirements will be gathered in four major categories, as follows:

- 1) Must have (Mo): The requirements that are critical and must be applied to a product as a matter of priority. Even if just one of them is not taken into account, the release version is considered to fall short of expectations.
- 2) Should have (S): Requirements that are important but not critical for the release. Such requirements are not very sensitive to time.
- 3) Could have (Co): The requirements are desirable but not mandatory for the release.
- 4) Won't have (W): These requirements are considered the least critical or may not correspond to the product strategy at all. They can be ignored and be revised for future releases.

Moreover, each functional requirement is numbered (so as to be uniquely identifiable). Considering all aspects presented above, we collected the functional requirements specific to SAQ tool in Chapter Functional Requirements.

2.2. Non-Functional requirements design methodology

This section aims to collect the non-functional requirements (NFR) that the SAQ application should meet. Whereas functional requirements define what a system should do, non-functional requirements specify how the system must work.

Moreover, non-functional requirements are those characteristics which describe how the system should behave and the potential constraints upon the system behaviour.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

In Figure 1, below The Open Group Architecture Framework (TOGAF) [TOG18] categories of non-functional requirements are presented.

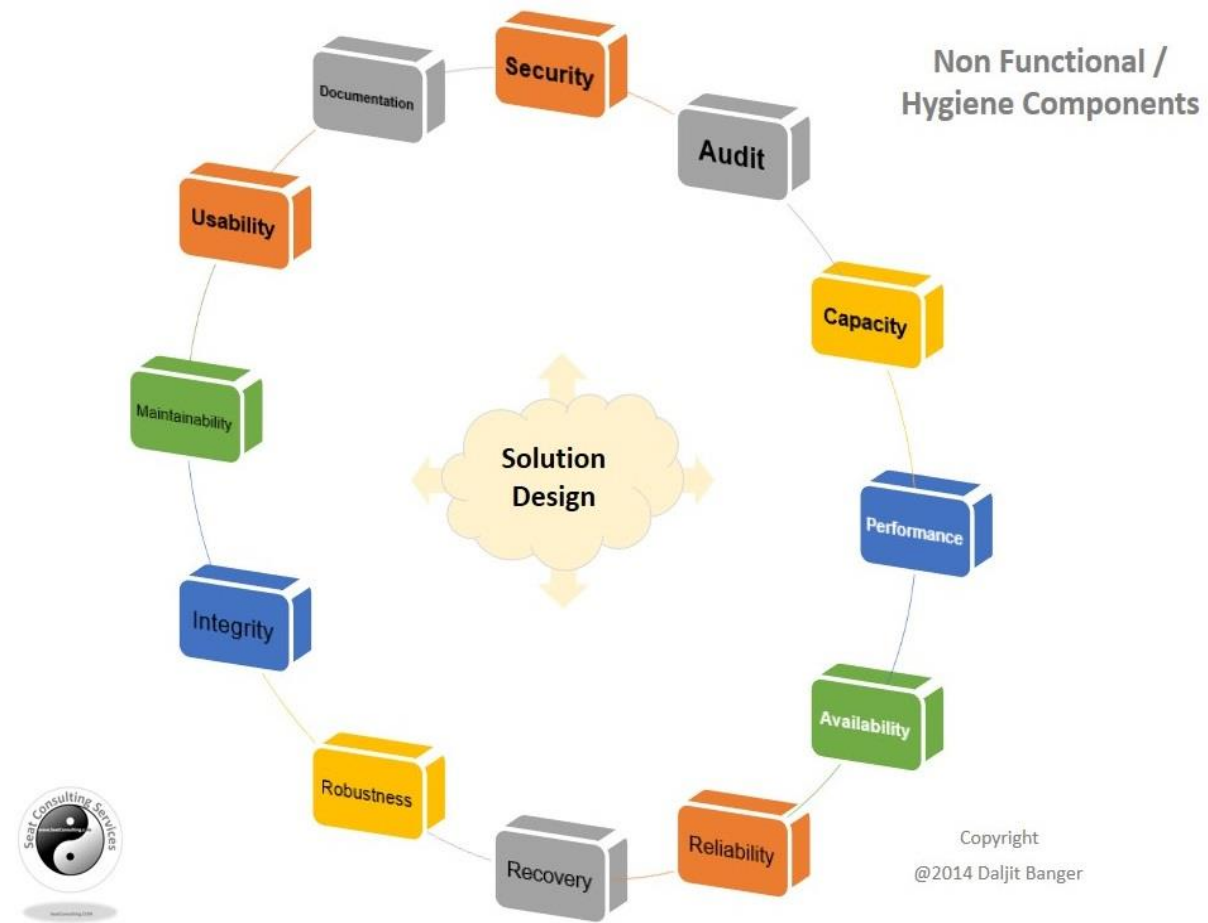


Figure 1 TOGAF categories for non-functional requirements | Source: <https://dalbanger.wordpress.com/>

Similarly, to FRs, the approach for non-functional requirements assumes that NFRs are associated to each SAQ requirement and are formalised in a unitary form as presented in Table 5 Non-functional requirements.

NFR ID	Description	MoSCoW	Chapter
NFR1	Maintainability - The questions from the questionnaires and tests of the system are not hardcoded but can be dynamically updated in each software release	M	Chapter number.

Table 5 Non-functional requirements template

Each NFRs has a unique identifier and all information collected from technology providers are available in Chapter Non-Functional requirements.

2.2.1. Security overview

The security view presents the characteristics of the system in terms of confidentiality, integrity and availability. This is recognised as CIA Triad in information security [MAT11].

The CIA Triad is a central part of ISO/IEC 27001:2019 [ISO19] the international standard that describes best practice for an information security management system.



Figure 2 CIA Triad | Source: <https://wizardcyber.com/>

The overall security takes into consideration the well-established CIA triad. The CIA triad (Figure 2) is a well-known concept in security that defines the security of a system. Some people define the CIA triad as the three pillars of security, all equally important.

Confidentiality. This pillar assures that the information in a computer system can be only accessed by the people that should view it. Confidentiality can be achieved through using all the methods described below (they should be used together).

- **Authentication** – an application should use unique name accounts that authenticate a user based on at least one authentication factor. The user account should be named and should uniquely identify that user. Anonymous accounts like *root* should be disabled, because if more people have access to the password there won't be a trail of who did what. Authentication can be done using one, 2FA (2 Factor Authentication) or more factors. A user can be authenticated in system based on:

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- What he knows – a password
- What he has – a token or a key card
- What he is – biometrics (fingerprint, iris etc.)
- **Authorisation** – after a user is authenticated the system must define what can the user do, what the user is authorised to do. This authorisation is maintained through access rights. Access rights will follow the least privilege principle. A user is given only the access necessary to do his job.
- **Encryption** – this method is used to make sure the data is safe from prying eyes. Encryption is a two-way mathematical function that allows the data to be rendered unreadable for the people without the decryption key. Encryption should be used for both data at rest (stored) or data in transit (data transmitted over the internet). The two methods explained above can't be implemented if encryption is not used. For example: if we try to authenticate someone by sending the password in an unencrypted manner over the internet the entire system will be compromised, because if the password is compromised that user account will be compromised.

Integrity. This pillar assures that data is accurate and trustworthy. We need to know that the data we're viewing or modifying is the actual data from the system. The same principle applies in reverse, we need to make sure that the data we send to the server is the data we modified. Integrity is assured using:

- **encryption** – we make sure that the data we transmit over the internet is encrypted and can't be read or modified by other people.
- **hashing** - this method assures the integrity of data per say, but can't work without other methods presented here. Hashing is a mathematical collusion resistant one-way function that presents a digest¹ of a message. If the message is changed that digest is changed. A property of a hash algorithm is that any small change in the initial message will produce a major change in the hash. Integrity is an innate property of Public Key Infrastructure (PKI), digital certificates, that we'll be used throughout the project.
- **Authentication and authorisation** are also used here, because only an authenticated user should be able to access the system, and also the system should be accessed based on the user rights.

Availability. This pillar assures that the system is accessible for the people that need access to it for as much time as possible. It doesn't matter how secure a system is if you can't have access to it, the system doesn't work.

Availability is achieved by putting in place redundancies both for:

¹ A message digest is a cryptographic hash function that accepts a message and creates a unique string of numbers that will ensure no one else modified the message.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- **Capacity** – assuring that the right number of concurrent users can use the system-of-systems
- **Protection against Distributed Denial of Service (DDoS)** – protection against malicious actors that might want to flood it with unnecessary requests to make it unavailable.
- **Backups** – system backups are very important because if a breach occurs and all the historic data is deleted/encrypted by ransomware the system becomes unavailable.
- **Logs** – logs are applicable for the system as whole, not only in the availability part. We mention it here because it's an integral part of business continuity. Logs allow system administrators to monitor what's happening in real time or what has happened at a point in time [SHO09].

2.3. Personal data collected by the application

The SAQ application will collect only the data necessary for account management, as shown in Table 6. Since all the responses will be anonymous the application will store personal data of the system administrators and questionnaire creators. **The SAQ application won't store any personal data of questionnaire respondents.**

Data collected	Purpose
Email	Account management
Full name	Account management
Company/Institution	Account management
Job title	Account management

Table 6 Personal data collected by SAQ application

Statistics

The SAQ application will generate **anonymous** overall statistics regarding information per questionnaire and overall:

- Medium score
- The most troublesome areas that need improvement
- Average time for improvement (based on the time since a user has filled in another self-assessment)

3. Functional Requirements list

The functional requirements and non-functional requirements for the application were derived from the Grant Agreement specifications. Please refer to Annex 1 – Correspondence matrix that maps all the requirements for the Grant Agreement with the FRs we defined here.

The list below details only the main application functionalities. All the applications flows and FR are detailed in chapter 5.

FR ID	Description	MoSCoW	Chapter
FR1	The application will allow user creation through the interface	M	5.1
FR2	The user will validate his/her account otherwise it will be deleted	M	5.1
FR3	The application will allow the questionnaire definition through the interface	M	5.2
FR4	Each application questionnaire will allow to choose between 2-5 options	M	5.2
FR5	The application will allow the publishing of the questionnaire and generate a link to be used by users to respond.	M	5.3
FR6	The user will respond to the questionnaire in an anonymous way	M	5.4
FR7	The user will receive a score and a security self-assessment.	M	5.4.3
FR8	The application will generate complex campaign statistics.	M	5.5
FR9	The link to the security self-assessment questionnaire will be published on EU survey website.	M	5.4

Table 7 Functional requirements list

4. Non-Functional requirements list

The functional requirements and non-functional requirements for the application were also derived from the Grant Agreement specifications. Please refer to Annex 1 – Correspondence matrix that maps all the requirements for the Grant Agreement with the FRs we defined here.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

The list below details only the main application functionalities. All the applications flows and NFR are detailed in chapter 5.

NFR ID	Description	MoSCoW	Chapter
NFR1	Administrator will not see any questionnaire data.	M	5.1
NFR2	The user password will be hashed, so no other person besides the user will have access to the password.	M	5.1
NFR3	The application will be hosted using HTTPS with all content encrypted.	M	5
NFR4	The application will contain only vetted users	M	5.1
NFR5	Define the content of the questionnaire taking into account the research findings from WP2 and the requirements from WP3.	M	6
NFR6	Dissemination of the online cybercrime vulnerability self-assessment tool to national SME associations by M20 with 100 responses from SMEs and CSOs to the online self-assessment questionnaire before the end of the project.	M	6

Table 8 Non-functional requirements list

5. Application Flows

The application will use HTTPS with authenticated sessions for admin and creator user types. An admin and creator must be authenticated in the application. A session will expire after 1 hour of inactivity. The application will allow the questionnaire response to be done anonymously using a link generated by the application.

Table 9 defines the entities used throughout this document:

Entity name	Description	Relationships with other entities
User type: Admin	Admin is the default user in the application. Admin is the application administrator and doesn't have access to questionnaire data.	Admin can make a new creator account, can change questionnaire ownership, and campaigns ownership etc.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

		Admin doesn't have access to campaign, questionnaire, and response data. Admin can reset passwords for other accounts.
User type: Creator	Creator account is capable of creating questionnaires, campaigns, and view statistics.	A creator will be able to define questionnaires, create campaigns, view security assessments and statistics. A creator can only see the data he owns (the campaigns he/she is the owner of).
Questionnaire	The questionnaire represents a set of questions with choices.	A single questionnaire is part of a campaign. Different campaigns can contain the same questionnaire.
Campaign	A campaign contains a questionnaire, has a state (Active or Closed) and can accept responses.	A campaign has one questionnaire attached to it. A campaign has more anonymous responses attached to it. A closed campaign doesn't accept responses. A campaign has statistics.
Response	A response represents the anonymous user response to a campaign.	A response is associated with a single campaign.
Individual security assessment	An individual security assessment is automatically generated and shown to an anonymous respondent after he/she responded to a campaign.	An individual security assessment is automatically generated to a response. Each response in a campaign has an automatically generated security assessment.
Statistics	Statistics are generated per campaign	Each campaign has one set of statistics attached to it. Statistics can be generated for both Active and Closed campaigns.

Table 9 Application entities

5.1. Account management

5.1.1. User creation

Admin will receive through internal channels (email) a request for user creation (to be defined in a procedure). Admin logs to the application and creates the user as depicted in Figure 3.

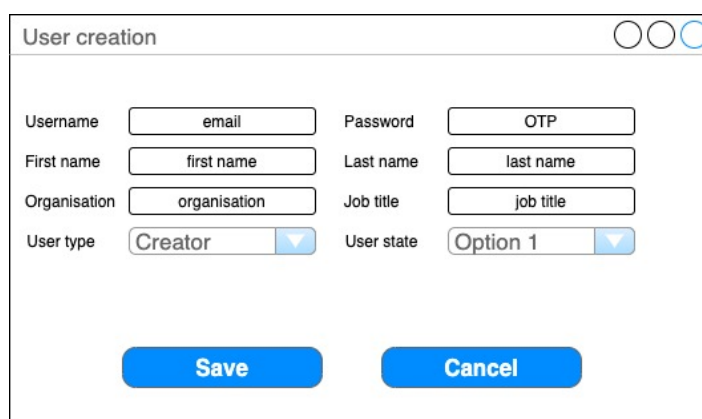


Figure 3 User creation

Figure 3 explanation:

- Username – this field will consist of user’s email. Field validation: check if the email is in the form of xxxxx@mailprovider.xxx.
- Password – the application **will generate a random password** for the user. The password will respect the password requirements for the entire app (listed in 5.1.2). The password field will accept inputs up to 100 in length.
- First name - – alphanumeric 50 characters, input should be sanitized against special characters like ‘, @, \$, %, ^, &, *’
- Last name – alphanumeric 50 characters, input should be sanitised against special characters like ‘, @, \$, %, ^, &, *’
- Organisation – alphanumeric, 80 characters, input should be sanitised against special characters like ‘, @, \$, %, ^, &, *’
- Job title - alphanumeric, 80 characters, input should be sanitised against special characters like ‘, @, \$, %, ^, &, *’
- User type – combo box automatically filled in to Creator. **The combo box is disabled.**
- State – combo box. This field can take the following values: New, Active, Re-Active, and Deactivated. When a user is created the state will be automatically set to New and the combo will be disabled – admin won’t be able to change it during the initial user creation process.
- Admin will be able to press Save or Cancel button. Cancel button will cancel the entire operation and no user will be created. Pressing Save button will activate the user validation flow.

5.1.2. Validation

After user is created the flow from Figure 4 will be implemented:

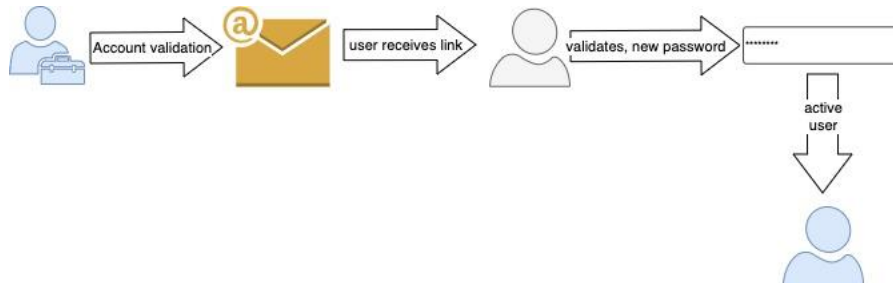


Figure 4 User validation

Flow details:

- Step 1: after Admin presses the Save button an email with a validation link (OTP) will be generated. This link will be valid for 7 days.
- Step2: User receives the email and clicks on validate.
- Step3: The user will be sent to the application where he/she will have to change the password. If the user doesn't complete this step the account will still remain in **New** state. After the password is changed, the account will change to **Active** state.

Other considerations:

- All accounts with New state will be automatically deleted after 7 days if not activated.
- Admin will be able to deactivate a user, **NOT delete**. When a user is re-activated (state is changed from Deactivated to Re-Activated) the application will resume the flow from step 2. In this case, after the user will change the password it's state will change to Active. All accounts with Re-Activated state will be automatically put in Deactivated state if not activated by user within 7 days.
- Password minimum requirements:
 - o Minimum 12 characters
 - o Must contain at least one letter
 - o Must contain at least one number
 - o Must contain at least one special symbol
 - o The password field will accept inputs up to 100 in length
- Password storage security requirements:
 - o Passwords **won't** be stored in clear text
 - o Password will be stored using a cryptographic secure hash generated with an accepted Hash algorithm like: SHA-2, SHA-3 etc.
 - o Administrators won't be able to change passwords.
 - o Only the user will be able to change his own password.

5.1.3. User authentication

Users will be able to authenticate using a username and password, described in Figure 5:

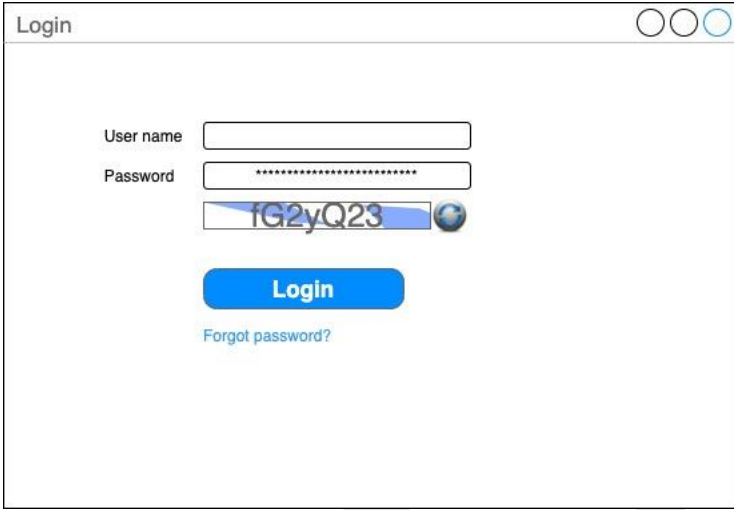


Figure 5 User Authentication

Login form (Figure 5) details:

- Username – user will fill-in username
- Password – user will fill-in password
- Captcha – the user won't be logged in if captcha is incorrect.
- Refresh captcha – the user will have the option to refresh captcha
- Login button – when user presses login he will either: **be logged in** if all fields are correct (username, password, captcha) or **not** (if any error occurs in any of the three fields). The system will display the following error messages:
 - If captcha is incorrect the application will show an error message “incorrect captcha, please try again” – at this stage the form will be pre-filled with the username and password already provided and a new captcha will be generated.
 - If either username and/or password are incorrect the application will display a generic message “Username or password incorrect!”.
- Forgot password (question) - If the link is pressed a new form will be shown that will contain only email field and Reset button. After reset button is pressed the user will receive the message: “An email was sent to the email provided!”. Even if the email is not associated with a user in the system, the application **will not disclose** this information in a message, because it can be used by an attacker to see if a certain email address has an account in the application.

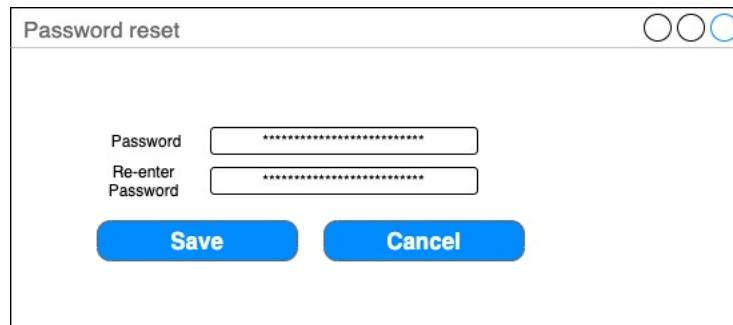
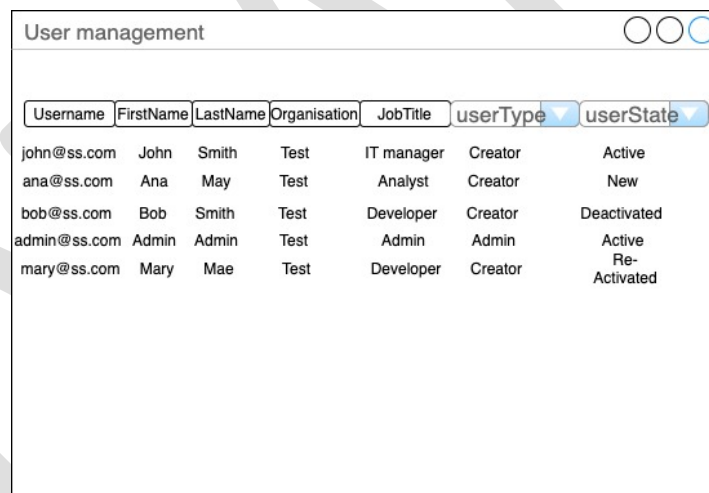


Figure 6 Password reset

- The user will have to click on the reset link received on the email and he will have to enter the new password twice (Figure 6), verifying that the passwords are the same. The password will respect the password rules defined above.

5.1.4. User administration

Admin will see the entire list of users and will be able to filter/search them using any field (Figure 7).



Username	FirstName	LastName	Organisation	JobTitle	userType	userState
john@ss.com	John	Smith	Test	IT manager	Creator	Active
ana@ss.com	Ana	May	Test	Analyst	Creator	New
bob@ss.com	Bob	Smith	Test	Developer	Creator	Deactivated
admin@ss.com	Admin	Admin	Test	Admin	Admin	Active
mary@ss.com	Mary	Mae	Test	Developer	Creator	Re-Activated

Figure 7 User Management

Figure 7, details the user list:

- Admin will be able to search using: user name, first name, last name, organisation, job title.
- Admin will be able to filter using: the user type and user state combo boxes
- Double clicking on the row containing the details about a user will send Admin to the Modify user interface (Figure 8).

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

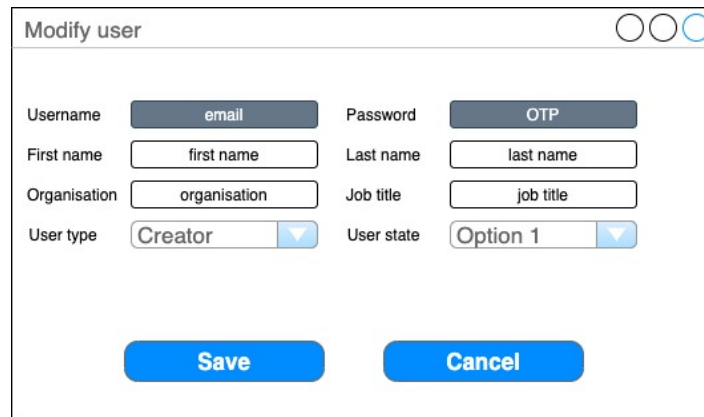


Figure 8 User Modification by Admin

Admin will be able to modify user (Figure 8) with the following constraints:

- Username (**field disabled**) - can't be modified, if there is a mistake in the email the current user will be deactivated and another one created.
- Password (**field disabled**) – Admin can't modify the password, only the user through his profile (password change) or through a reset link (password reset)
- First Name, Last Name, Organisation, Job title – Admin can modify these fields
- User type – Automatically filled to Creator. **The combo box is disabled.**
- User state – Admin can only change to Deactivated and Re-Activated (the other two options will be disabled).
- Save button – saves changes
- Cancel – cancel changes

Behaviour of user state combo-box:

- User state can have one of the following values: New, Active, Re-activated and Deactivated
- When the user is first created by Admin the user state will be automatically filled in to New and combo-box deactivated.
- After the user validates his account the state of the user will be automatically changed to Active.
- Admin will be able to change the user with states Active or Deactivated.
 - o Admin can change Active to Deactivated
 - o Admin can change Deactivated to Re-Activated
- Once the user is in Re-activated state the user will have to activate his account and the app will automatically change the state to Active
- All users with New state will be automatically deleted after 7 days if not activated
- All users with Re-activated state will be automatically put in Deactivated stated if not activated in 7 days.

5.1.5. User profile

The following are considerations for user or creator behaviour:

- A Creator:

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Can change some of his personal data. He will be able to modify (Last Name, First Name, Organisation, Job title).
- The creator **can't** modify: email, password field, user type and user state.
- The creator can change his password by: using the reset link (detailed in Figure 6) or by pressing the password change button. Once the password change button is pressed the password reset form will be displayed. Figure 9 details:
 - The creator will have to enter the current password and the application will check. If that won't match the user won't be able to change his password.
 - The application will verify the new password and re-enter new password inputs are the same. The password will respect the password rules defined above.
 - If all fields are correct the new password will be changed.

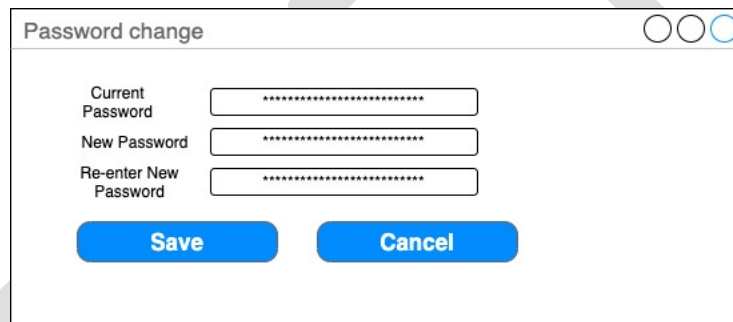


Figure 9 Password change

- Can create questionnaires
- See all answers/reports to a questionnaire he created, without modifying the answers.
- See all statistics for the questionnaires created.
- Admin:
 - Can create accounts, deactivate them (everything that was detailed in this section)
 - Can change the owner of a questionnaire to another user with type creator.
 - Admin **can't** change a creator's password
 - Admin **can't** view any answers to questionnaires, reports, statistics.

5.2. Questionnaire design and management

5.2.1. Questionnaire design list

A **creator** will go to the questionnaire list, Figure 10.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

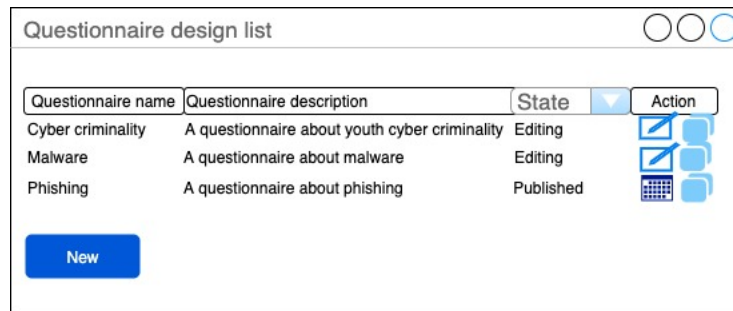


Figure 10 Questionnaire list

Figure 10 details the questionnaire list:

- The creator will be able to search using: questionnaire name, questionnaire description
- The creator will be able to filter using: state combo-box.
- Depending on the **questionnaire state** the user will have the following actions:
 - o Questionnaire is in **Editing** state: – the user will see the **Edit and Copy** buttons. Pressing **Edit** will send the user into the questionnaire design interface, where he can edit it. Pressing the **Copy** will prompt the user to choose a new name and description and create the new questionnaire. The name will be prefilled with the old name + Copy word. All old questionnaire data is copied as is and the new questionnaire will be put in Edit mode.
 - o Questionnaire is in **Published** state – the user will see the **Campaign and Copy** buttons. Pressing the **Campaign button** will send the user to the continuous evaluation campaign module, detailed in 5.3. Pressing the **Copy** button will prompt the user to choose a new name and description and create the new questionnaire. The name will be prefilled with the old name + Copy word. All old questionnaire data is copied as is and the new questionnaire will be put in Edit mode. The data regarding the answers won't be copied and the new questionnaire will be put in Edit mode.
- A published questionnaire can't be edited.
- Only Admin is able to delete a questionnaire.
- Only Admin can change the owner of a questionnaire.
- Pressing the New button will open the new questionnaire interface depicted below (Figure 11).

5.2.2. New questionnaire

Pressing New button from Figure 10 will open the New questionnaire interface, detailed in Figure 11 :

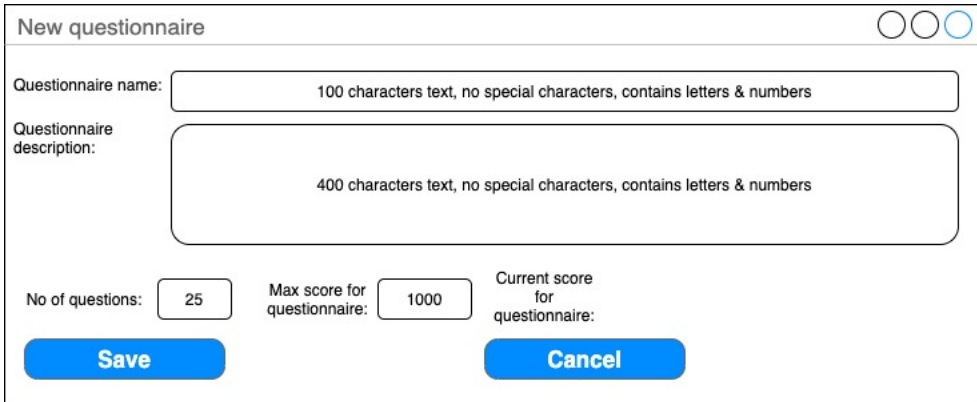


Figure 11 New questionnaire

Figure 11 details the new questionnaire interface:

- Questionnaire name – field containing max 100 characters, letters and numbers
- Questionnaire description – field containing max 400 characters, letters and numbers
- No of questions – number between 1-50
- Max score – number between 1000-5000 pre-filled with 1000.
- Cancel button will cancel the questionnaire creation.
- Save will save the questionnaire and the following interface (Figure 12) will be shown:

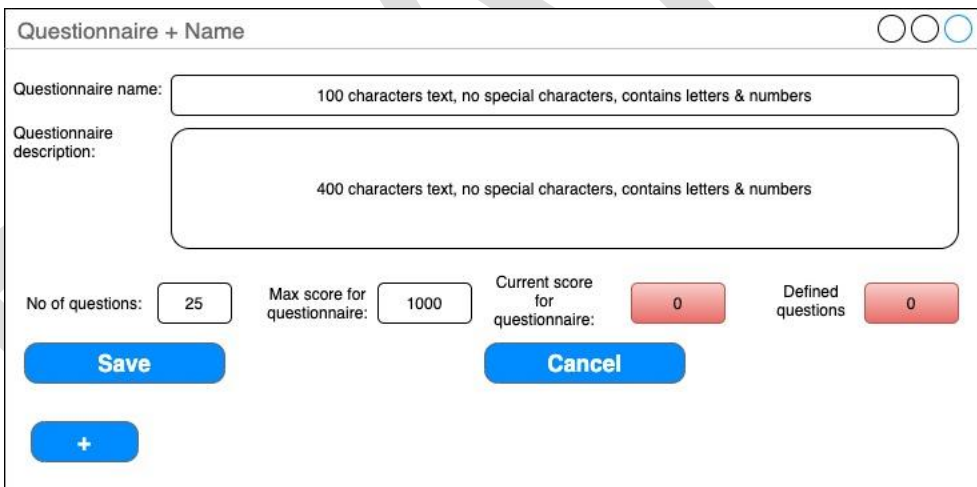


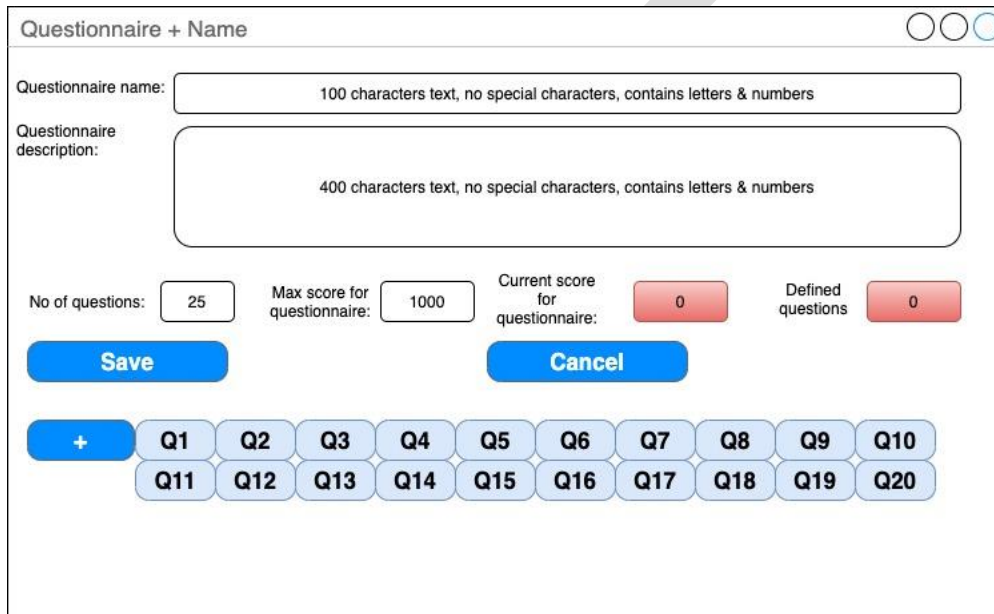
Figure 12 Saved Questionnaire

The interface from Figure 12 is shown after the questionnaire was saved. The user will be able to change the questionnaire name, description at any point. The user won't be able to change the number of questions to less if there are questions defined. Example: the questionnaire has 20 questions defined; accordingly, the number of questions is set as 20. If the user wants to change the no of questions to 10, he will have to delete the questions he doesn't want and then change the no of questions field.

The interface will show previous fields (detailed in Figure 11) + new additional fields. The additional fields are detailed:

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Current score for questionnaire – the application will calculate the current score based on the max score of the questions defined. The score will be red until the max score of the questions will equal the max score for the questionnaire, then it will be marked with green. User can't edit this field.
- Defined questions – the application will show the current number of questions defined. The field will be red until the number of questions will equal the no of questions field, then it will be marked with green. User can't edit this field.
- Pressing the + button will add a new question. When a new question is added a Q field is shown so the user can seemly navigate through the questions, as shown in Figure 13.



Questionnaire + Name

Questionnaire name: 100 characters text, no special characters, contains letters & numbers

Questionnaire description: 400 characters text, no special characters, contains letters & numbers

No of questions: 25 Max score for questionnaire: 1000 Current score for questionnaire: 0 Defined questions: 0

Save Cancel

+ Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10
Q11 Q12 Q13 Q14 Q15 Q16 Q17 Q18 Q19 Q20

Figure 13 Questionnaire navigation

Pressing + will create a new question. The Q field will be created with the fields depicted in Figure 14.

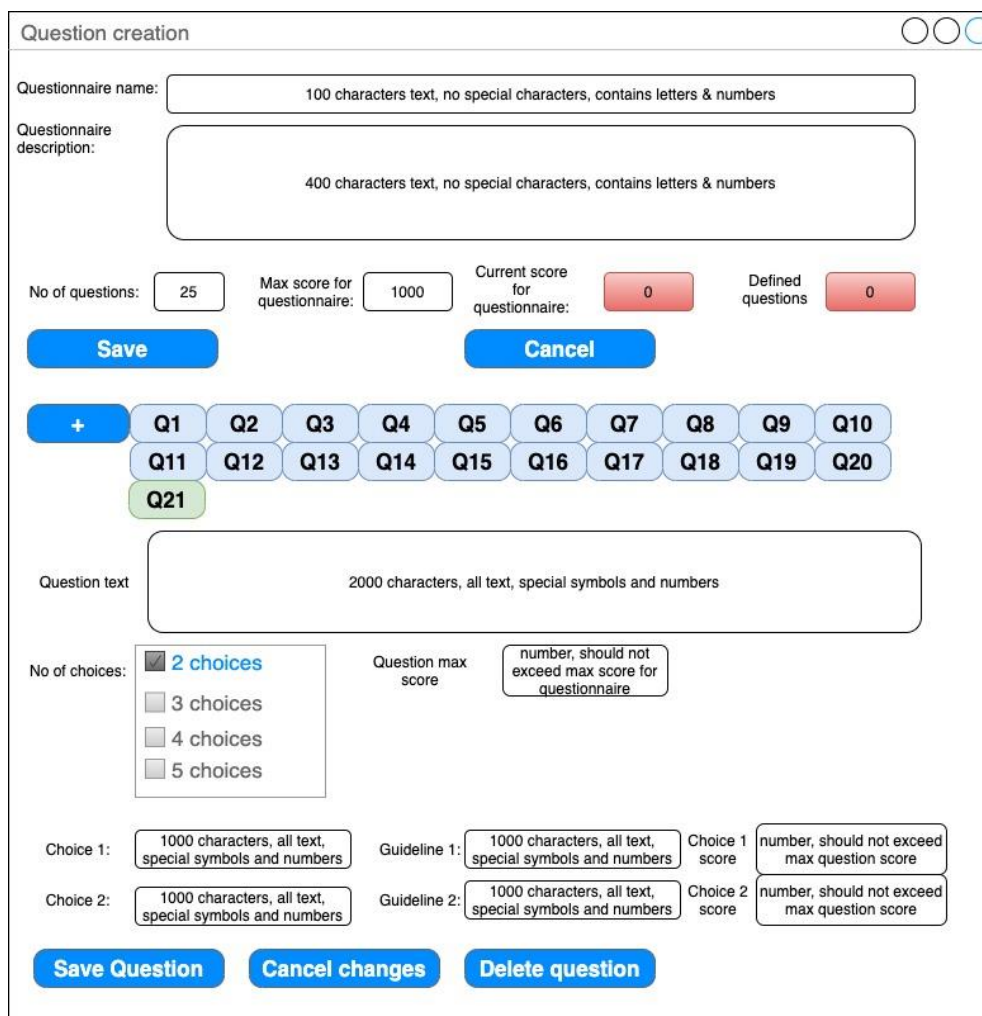


Figure 14 Question creation

Figure 14 question fields description:

- Question text – represents the text for the question. This field has 2000 characters: text, special symbols, and numbers.
- Question max score – represents the maximum score that can be obtained for this question which won't exceed the questionnaire max score.
- No of choices (between 2 and 5) – the user will have to pick from 2,3,4,5 values. After this value is chosen the application will create the appropriate choice rows, which can be 2 rows, 3 rows, 4, and 5 rows, each for each number of choices. The choice rows will contain the following fields:
 - o Choice X – X is the choice number (1,2,3,4,5). This field represents the text of the choice. This field has 2000 characters: text, special symbols, and numbers.
 - o Guideline X - X is the guideline number (1,2,3,4,5). This field represents the text of the guideline. This field has 2000 characters: text, special symbols, and numbers. Each choice will have a guideline.
 - o Choice score – the score of the choice. The application will check that a choice score doesn't exceed the max score defined for that question (not allowed to put

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

more than max score). If two answers will have the question's max score – a notice will appear, but the question can be saved.

- The user will be able to press the following buttons:
 - o Save question – saves the question
 - o Cancel changes – the question will revert to the previous state. If the question is new (meaning it has never been saved) and the user presses Cancel changes the application will delete that question.
 - o Delete question – deletes the question.
- After the user presses one of the buttons the current score for questionnaire and NoOfDefined questions will be updated. The Current score for questionnaire is calculated using the formula detailed in Equation 1:

$$\text{Current score for questionnaire} = \sum_{i=1}^n \text{Question max score}$$

Equation 1 Current questionnaire score

- Current score for questionnaire: will **add** all question max score fields for all saved questions.
- Defined questions: will show the total number of defined questions.
- n represents the total number of questions in the questionnaire.
- The user will be able to save all the changes and come back to the questionnaire.
- The **Publish** button will appear when the following conditions are met (Figure 15):
 - o User has defined all the questions – **No of questions** filed = **Defined questions** field
 - o And the score is correct - **Question max score** filed = **Current score for questionnaire** field.

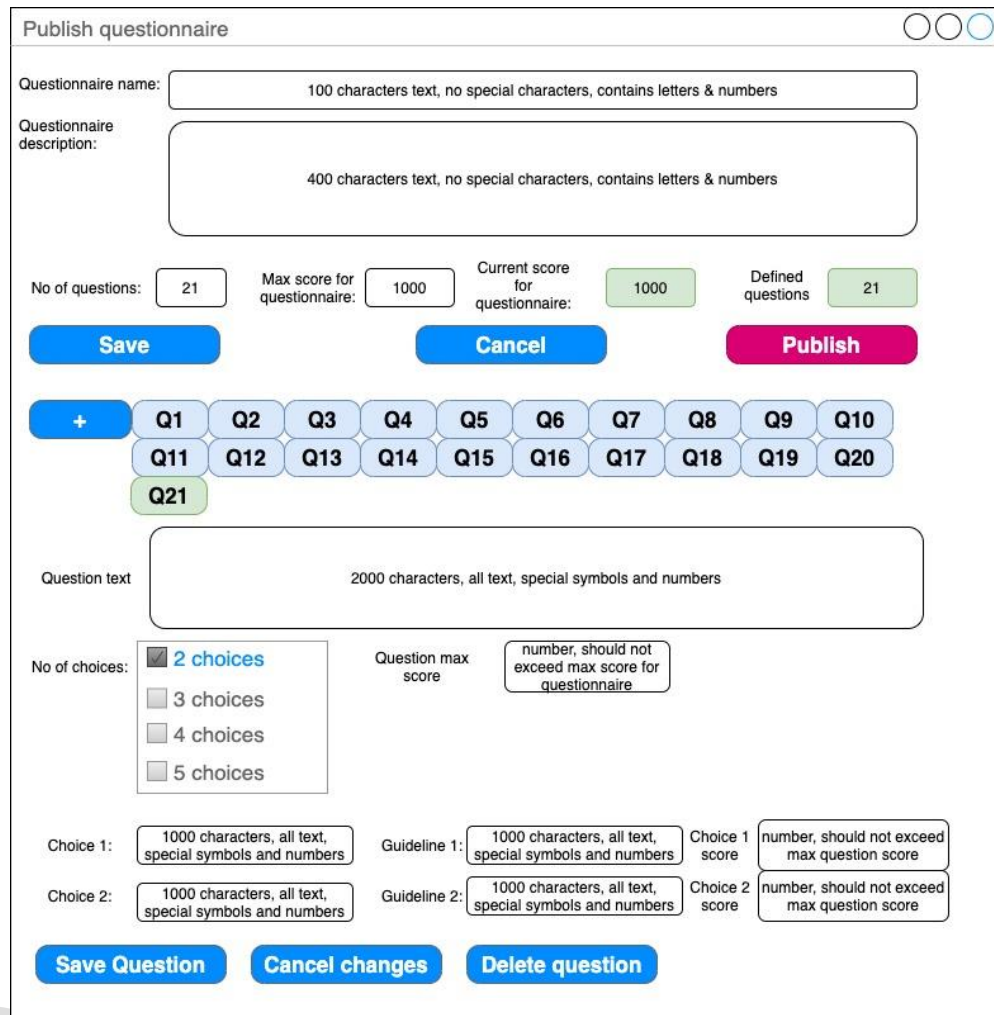


Figure 15 Publish questionnaire

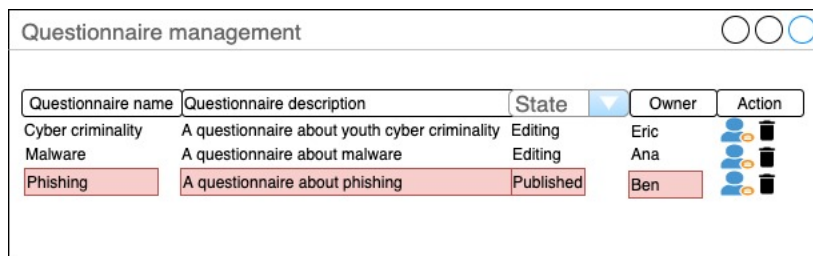
- If the creator presses the **Publish** button a message will be shown: “After publishing a questionnaire you won’t be able to edit it. Are you sure? (Yes and No buttons).
 - o If No is pressed the questionnaire won’t be published and the creator will be reverted to the previous screen, Figure 15.
 - o If Yes is pressed the questionnaire is published (the state of the questionnaire is changed to published). The creator will be reverted to the Questionnaire list screen, Figure 10. In this state the user won’t be able to change the questionnaire at all only to view it.

5.2.3. Admin questionnaire menu

Admin will be able to Delete an entire questionnaire and associated data or change the owner of a questionnaire. Admin will not be able to see any questionnaire data or change data.

The only information available to Admin are shown in Figure 16:

D4.2 [Cybercrime vulnerability self-assessment questionnaire]



Questionnaire name	Questionnaire description	State	Owner	Action
Cyber criminality	A questionnaire about youth cyber criminality	Editing	Eric	
Malware	A questionnaire about malware	Editing	Ana	
Phishing	A questionnaire about phishing	Published	Ben	

Figure 16 Questionnaire management admin

Figure 16 details:

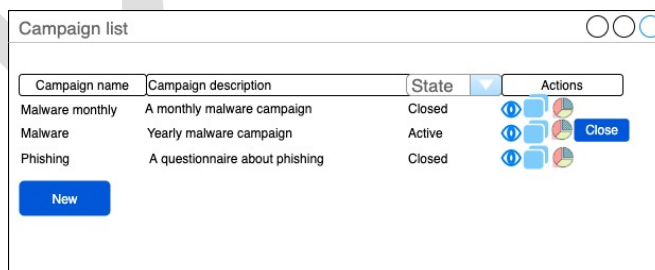
- Double clicking on a row does nothing.
- The owners Marked with red are users whose **state isn't Active** and Admin will have to change the owner.
- Pressing Owner button will show a dialogue with all active users with creator role and Admin being able to choose just one and press ok. This will change the owner and it will remove the red mark-up from the owner's name. **Changing the owner of a questionnaire will also change the owner for all the campaigns that questionnaire is a part of, please refer to section 5.3.1.** Admin will be able to change the owner for other questionnaires, but the application will mark the ones where the owner is not active.
- Pressing Delete will delete the questionnaire and all its content: questions, campaigns, responses, and statistics etc.

5.3. Campaign

This menu will be accessible to creators. Only Published questionnaires can be part of a campaign. One questionnaire can be part of multiple campaigns, but a campaign contains only one questionnaire.

5.3.1. Campaign list

A creator will go the campaign list and he/she will see only the campaigns she/he's an owner of, Figure 17:



Campaign name	Campaign description	State	Actions
Malware monthly	A monthly malware campaign	Closed	
Malware	Yearly malware campaign	Active	Close
Phishing	A questionnaire about phishing	Closed	

New

Figure 17 Campaign list

Figure 17 details the questionnaire list:

- The creator will be able to search using: Campaign name, Campaign description
- The creator will be able to filter using: state combo-box

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Depending on the **campaign state** the user will have the following actions:
 - o Campaign is in **Active** or **Closed** state: the user will see the **View, Copy, and Statistics actions**. Pressing **View** will send the creator into Campaign Viewing mode, 5.3.3. Pressing **Copy** will prompt the user to choose a new name and description and create the new campaign. The name will be prefilled with the old name + Copy word. All old campaign data is copied and the new campaign will be put in Editing mode. Pressing **Statistics** will send the creator to Statistics module 5.5.
 - o Campaign is in **Active** state: the **Close** button will be visible. Pressing the **Close** button, the following actions will happen:
 - The campaign state is changed to Closed
 - The Close button will disappear
 - The campaign won't accept new answers – the link will be disabled.
- A Closed campaign can't be edited.
- Only Admin is able to delete a campaign and change the campaign owner.
- Pressing the New button will open the new Campaign creation interface depicted below, in 5.3.2

5.3.2. Campaign creation

Pressing the new button (Figure 17) will show the campaign creation screen, depicted in Figure 18.

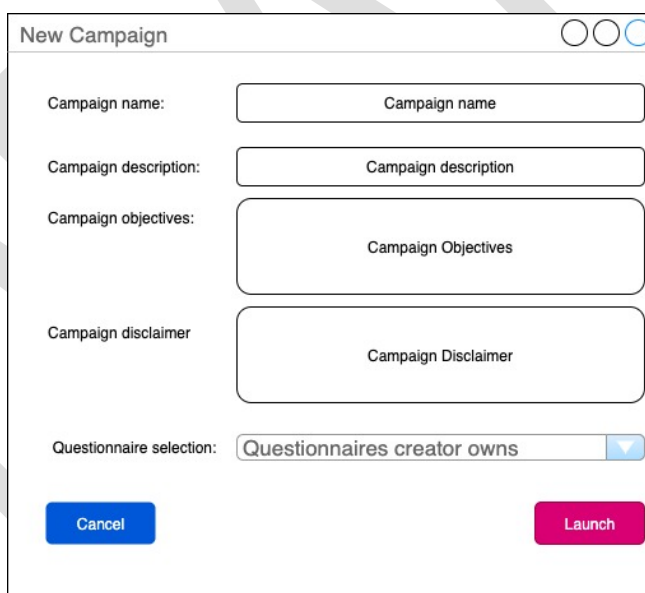


Figure 18 New campaign

Figure 18 details the screen for new campaign:

- **Campaign name** – name of the campaign
- **Campaign description** – description of the campaign
- **Campaign objectives** – a text field of 2000 characters that will contain free text about the campaign objectives.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- **Campaign disclaimer** – a text field of 2000 characters that will contain free text about the campaign disclaimer. This field will contain information about GDPR, data processing etc.
- **Questionnaire selection** – the creator will select a questionnaire that will be part of the campaign by choosing from combo. The combo-box will be populated with the names of the questionnaires the creator is an owner of. **Only one questionnaire can be part of the campaign while the same questionnaire can be part of multiple campaigns.**
- **Start date** – not visible in form, will be filled automatically when the Launch is pressed.
- **End date** – not visible in form, will be filled automatically when the Close campaign button is pressed.
- **Owner** – not visible in form, the owner will be automatically filled with the user id of the creator that made it.
- **Cancel** – will cancel any changes and send the user to the screen depicted in Figure 17.
- **Launch** – Pressing this button will Launch the campaign. When pressed the system will show a warning: “Launching a campaign will not allow any modification. Please verify the scheduling preferences and the number of users selected. Are you sure?” (Yes and No options).
 - Pressing No – will not do anything and will revert to Figure 17
 - Pressing Yes – will launch the campaign and the following actions will be performed:
 - the Campaign state will be changed to Active.
 - The system will automatically set the Start date of the campaign to current date and time
 - The system will leave the End Date blank.
 - The system will generate the Campaign Link that will be shared using other channels. This link will be visible in the viewing section.
- Other mentions:
 - The owner of the campaign will be automatically filled in to the username of the creator that design it.
 - When Admin changes the owner of a questionnaire, depicted in section 5.2.3, all the campaigns associated with that questionnaire will be transferred into the ownership of the new creator.

5.3.3. Campaign viewing

Pressing the View button from Figure 17 will show the following interface (the View button visible for Active and Closed campaigns).

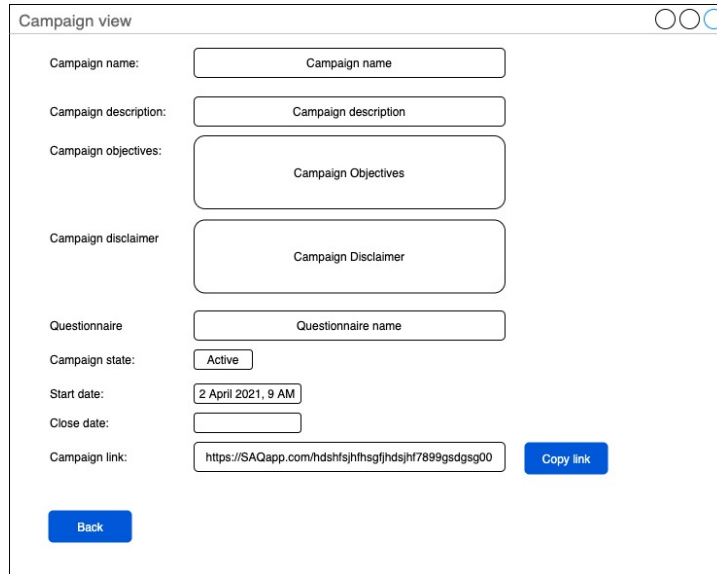


Figure 19 Campaign viewing

All the fields from Figure 19 are **Read only**. The creator will be able to see an overview of the campaign as follows:

- Campaign name – the name of the campaign
- Campaign description – the description of the campaign
- Campaign objectives – the campaign objectives
- Campaign disclaimer – the campaign disclaimer
- Questionnaire name – the name of the questionnaire that is part of the campaign
- Campaign state – The state of the campaign
- Start date – the campaign start date
- End date:
 - if the campaign state is Active this field is blank
 - if the campaign state is closed the system will display the close date.
- Campaign link – The application will generate a link that will be used by anonymous users to respond to the campaign (details in section 5.4). This link contains the path in the application and a complicated random string generated at the end of the campaign so it can't be guessed by people that don't have the link.
 - If campaign is in Active state:
 - The link field will be white
 - The Copy button will be visible – Pressing this button will copy the campaign link to the clipboard.
 - If the campaign is in Closed state:
 - The link field will be grey (disabled). The user won't be able to copy it.
 - The Copy button won't be shown.
- Back button – will send the user to previous screen depicted in Figure 17.

5.4. Campaign response

The respondent will be an anonymous user that will receive the campaign link via different channels like: social media, the project web-site, email etc. **As per grand agreement requirements we will share this link on the EU survey website.** The campaign link is visible in the campaign viewing section, as detailed in 5.3.3.

The user will be able to respond to the campaign in anonymous mode. The user won't be logged in and won't have access to any application pages or menus besides the campaign form.

5.4.1. Response start

If the campaign is in Closed state the user won't be able to fill in the response and the following interface will be shown (Figure 20):

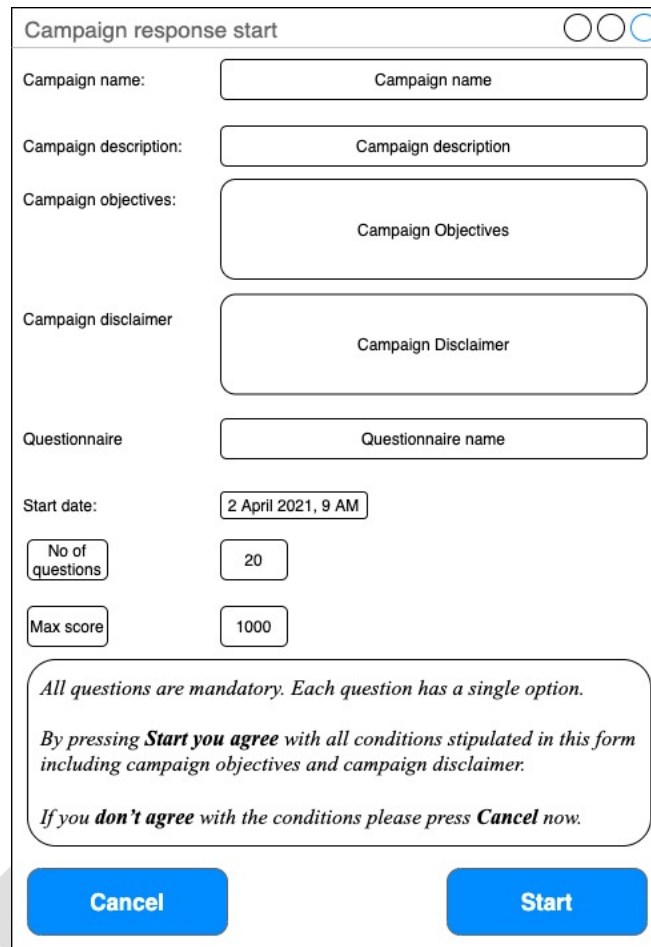


Figure 20 Campaign response closed state

Figure 20 details:

- The system will display the following disclaimer: "We're sorry the campaign <campaign name> has been closed and does not accept new answers". The system will fill in <campaign name> with the name of the campaign. If the campaign name is "Malware for LEAs" the text will be:
 - o "We're sorry the campaign **Malware for LEAs** has been closed and does not accept new answers."
- **Close tab** – when the user presses this button the tab will close.

If the Campaign is in Active state the following interface is shown (Figure 21):



Campaign response start

Campaign name: Campaign name

Campaign description: Campaign description

Campaign objectives: Campaign Objectives

Campaign disclaimer: Campaign Disclaimer

Questionnaire: Questionnaire name

Start date: 2 April 2021, 9 AM

No of questions: 20

Max score: 1000

All questions are mandatory. Each question has a single option.

*By pressing **Start you agree** with all conditions stipulated in this form including campaign objectives and campaign disclaimer.*

*If you **don't agree** with the conditions please press **Cancel** now.*

Cancel Start

Figure 21 Campaign response start

Figure 21 information is all read only and depicts:

- Campaign name – campaign name
- Campaign description - campaign description
- Campaign objectives – campaign objectives
- Campaign disclaimer – campaign disclaimer
- Questionnaire – questionnaire name
- Start date – campaign start date
- No of questions – the total number of questions from the questionnaire will be shown
- Max score – the maximum score of the questionnaire is displayed.
- The application will show in a marked box the following text:
 - “All questions are mandatory. Each question has a single option.*
 - By pressing **Start you agree** with all conditions stipulated in this form including campaign objectives and campaign disclaimer.*
 - If you **don't agree** with the conditions please press **Cancel** now.”*
- Cancel button – Will close the tab (the form closes nothing will be saved)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Start button – will start the questionnaire fill in depicted in next section (5.4.2).

5.4.2. Campaign questionnaire fill-in

Pressing the Start button depicted in Figure 21 will show the questionnaire fill in interface, detailed below (Figure 22).

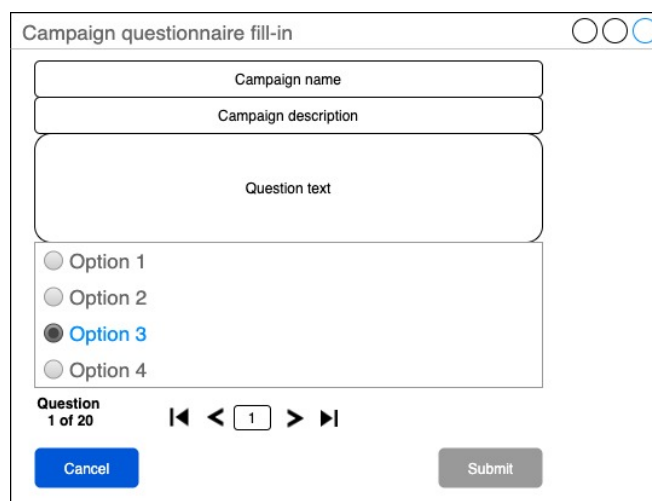


Figure 22 Campaign questionnaire fill-in

Figure 22 shows the questionnaire/response fill-in section:

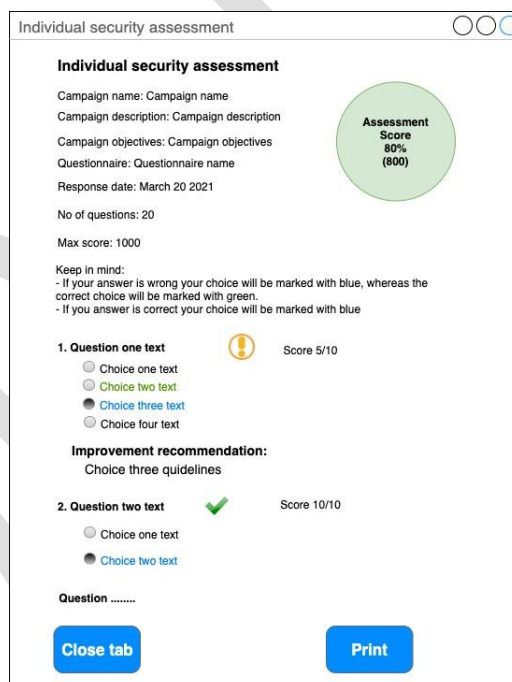
- Campaign name (read only) – campaign name
- Campaign description (read only) – campaign description
- Question text (read only) – the first question in the questionnaire
- Question options (checkboxes) – the options for the current question. When loaded **no** option is selected. The user needs to select an option. Once selected it will be checked. The question guidelines **won't be shown**.
- Questions **X** of **total** – this read only box will show the number of the current question out of all questions.
- Navigation bar (5 icons detailed in order from left to right):
 - o First question
 - o Previous question
 - o Current question – if the user fills in a number and presses enter that question will be shown
 - o Next question
 - o Last question
- Regarding the navigation bar the user will be able to move through questions and select the questions, skip some, and go back. Once a selection was made on a question it will be saved even if he navigates to another question.
- Cancel button – pressing cancel button will show a message box: “Are you sure you want to press cancel? All your progress will be lost (Yes and No buttons)”.
 - o Pressing Yes the tab will close
 - o Pressing No the message will disappear and the user resumes his work.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Submit button – this button is disabled until all the questions have been answered. After all the questions are answered the button will activate. The user will still be able to navigate back and forth through the questions. Once the submit button is pressed the user will be prompted with a message: “You are about to submit your response. This action can’t be undone! Are you sure? (Yes and No buttons)”
 - o Pressing Yes will submit the response and fill-in the response date. Immediately the application starts calculating the individual security assessment which will be immediately shown to the user, details in section 5.4.3.
 - o Pressing No the message will disappear and the user resumes his work.

5.4.3. Individual security assessment

The individual security assessment will be shown immediately after the user submits the response. The user will be shown the interface depicted in Figure 23.




Individual security assessment

Individual security assessment

Campaign name: Campaign name
 Campaign description: Campaign description
 Campaign objectives: Campaign objectives
 Questionnaire: Questionnaire name
 Response date: March 20 2021


No of questions: 20
 Max score: 1000

Keep in mind:
 - If your answer is wrong your choice will be marked with blue, whereas the correct choice will be marked with green.
 - If you answer is correct your choice will be marked with blue

1. Question one text  Score 5/10

Choice one text
 Choice two text
 Choice three text
 Choice four text

Improvement recommendation:
 Choice three guidelines

2. Question two text  Score 10/10

Choice one text
 Choice two text

Question

Close tab **Print**

Figure 23 Questionnaire individual security assessment

All the information **shown is read only** (Figure 23):

- The text “Individual security assessment”
- Campaign name – the name of the campaign
- Campaign description – description of campaign
- Campaign objectives – the objectives of the campaign
- Questionnaire – the questionnaire name
- Response date – response date

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Score obtained – the score obtained by the user after completing the questionnaire. The field will be formatted with colours: below 50% red, between 50%-70% yellow, and above 70% green. The score is calculated as a sum of all the individual questions score. The questions have different maximum scores based on the importance of the question, so there is no need for different weights to be used in the formula. The score will be shown in percentage and also in number. The percentage score is calculated as described in Equation 2.

$$\text{Questionnaire score} = \frac{\text{Score obtained}}{\text{Max questionnaire score}} * 100 \%$$

Equation 2 Questionnaire score calculation

- **Score obtained:** represents the sum of all the individual questions score. The score will be calculated and saved in a field in the database. It will be easier later on for the statistics module. The response score will be used for lots of statistics, so calculating this score only once will optimise the application and improve the response time of the statistics module.
- **Max questionnaire score:** represents the max questionnaire score.
- The score will be shown in % and in number value as shown in Figure 23. 80% represents Questionnaire score relative to the questionnaire max score (calculated in Equation 2) and 800 represents Score obtained.
- No of Questions – no of questions in the questionnaire.
- Max score – the questionnaire max score if all questions are correct.
- The following text note will be shown:
 - ” *Keep in mind:*
 - *If your answer is wrong your choice will be marked with blue and the correct choice will be marked with green. In this case two markings will be visible: the one with blue (your answer) and the one with green (the correct answer).*
 - *If you answer is correct your choice will be marked with blue, no other markings will be visible.*”
- The system will display each question text, question choices, score per question/max score per question, and for some questions the guidelines. All questions will be shown one after the other. Details about the information shown follow:
 - If the user has obtained the maximum score for that question, the question will be marked with a green ok icon (please refer to Figure 23, question two). The option the user chose will be clearly marked with blue (radio checked).
 - If the user has obtained less than maximum score per question, that question will be marked with a yellow! icon (please refer to Figure 23, question one).
 - The option the user chose – marked with blue (radio checked)
 - The correct option - marked with green (radio unchecked)
 - After the question options the following text will be shown:
 - The text: “Improvement recommendation:” (font bold)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- The contents of the guideline filed for the choice the user selected will be displayed. If the user selected choice 3, the contents for the guideline 3 will be shown.
- The questions will be presented one after the other in order. The user will be able to print and/or download the assessment.
- Close tab button – will close the tab
- Print button – will open the print dialogue where the user can print the assessment or save it.
- We might opt to add pagination and navigation bar before the buttons, we'll decide this aspect during implementation.

Depending on how much time the assessment takes to display, we might choose during implementation, to generate the assessment once and save it as a PDF in the database. This will improve the performance of the application. This section will be updated accordingly with the modifications done in the system implementation phase.

5.5. Campaign statistics

This module is accessible only to the users with creator role. The creator will see the campaigns he owns. The statistics module is accessible from the campaign scheduling interface, by pressing the Statistics button (as depicted in section 5.3.1, Figure 17).

Once the campaign **Statistics button** is pressed the campaign details and statistics will be presented. Because of the complicated formulas the campaigns statistics will be detailed in this document twice, as follows:

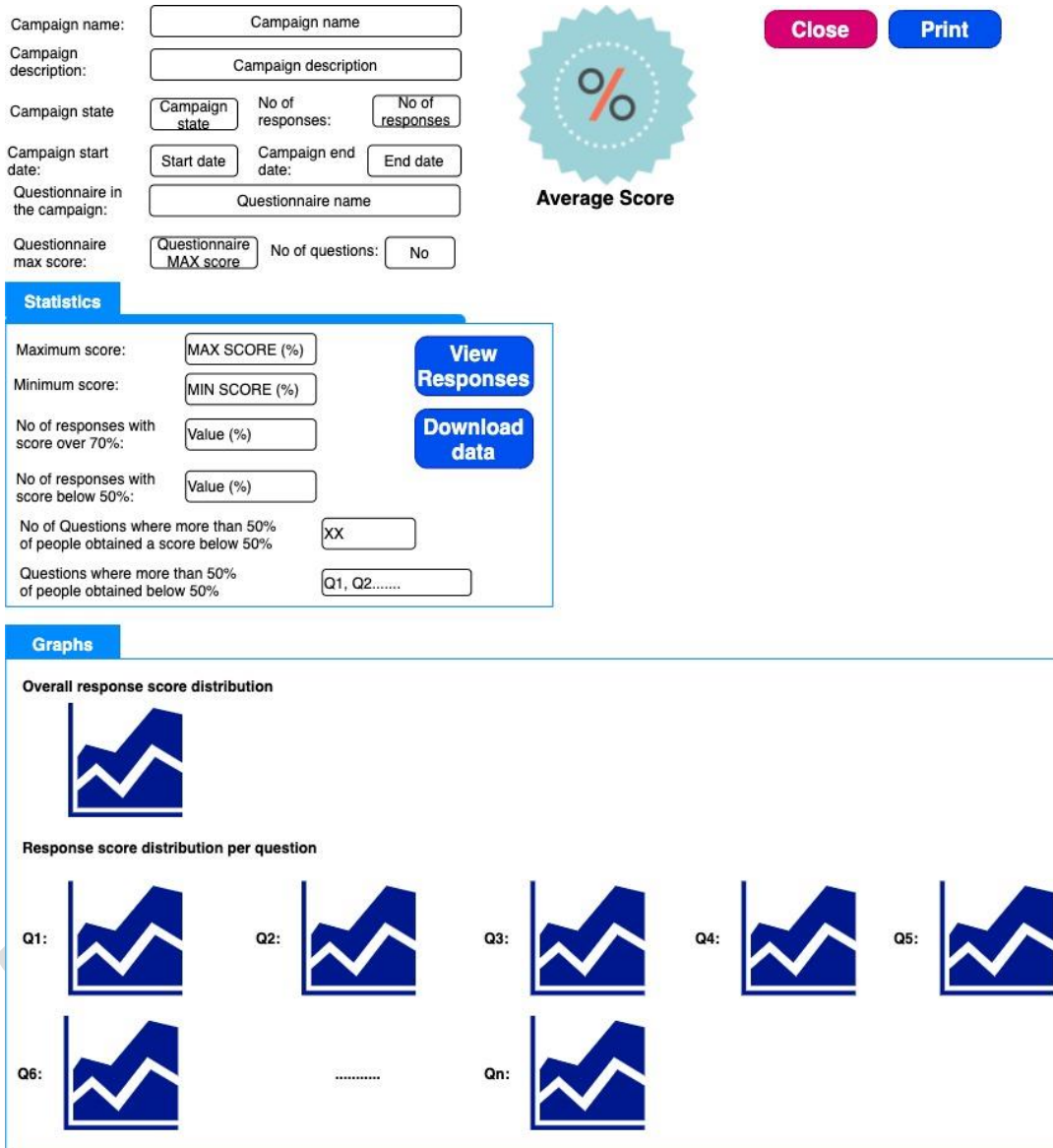
- **Design screen with formulas** - will present the fields and formulas for the statistics
- **Design screen with data** – will present a statistic form using mock-up data presented in this document.

Both design screens will show the same information, but mock-up data will be used for clarification and formula check.

The user will be able to see live statistics for an active campaign. The statistics data might take a lot of time to calculate, so during implementation we might choose to calculate them once and show an additional button to regenerate the statistics if new responses to the campaign were added.

This section will be updated accordingly with the modifications done in the system implementation phase.

5.5.1. Design screen with formulas



Campaign name:

Campaign description:

Campaign state: No of responses:

Campaign start date: Campaign end date:

Questionnaire in the campaign:

Questionnaire max score: No of questions:

Average Score

[Close](#) [Print](#)

Statistics

Maximum score: [View Responses](#)

Minimum score: [Download data](#)

No of responses with score over 70%:

No of responses with score below 50%:






No of Questions where more than 50% of people obtained a score below 50%:

Questions where more than 50% of people obtained below 50%:

Graphs

Overall response score distribution

Response score distribution per question

Q1:  Q2:  Q3:  Q4:  Q5: 



Q6:  Qn: 

Figure 24 Campaign statistics design screen with formulas

Below are explanations of every field and formula from Figure 24. All data presented is **Read Only**:

- **Basic campaign information:**

- Campaign name – campaign name
- Campaign description – campaign description
- Campaign State – The state of the campaign (Active or Closed)
- No of responses – no of responses per campaign (how many responses we have for the campaign)
- Campaign start date – campaign start date

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Campaign end date – campaign end date (for Active campaigns the end date will be filled in with N/A)
- Questionnaire in the campaign – the name of the questionnaire that is part of the campaign
- Questionnaire max score – the maximum score that can be obtained by correctly filling in the questionnaire
- No of questions – no of questions in the questionnaire
- Average score – This is the average score per round that will be shown in number value (percentage %). The field will be formatted with colours: below 50% red, between 50%-70% yellow, and above 70% green. The number value is computed as shown in Equation 3, whereas the percentage is computed as shown in Equation 4.

$$\text{Average score} = \frac{\sum_i^n \text{Score obtained}}{\text{No of responses in campaign}}$$

Equation 3 Average score per round

- i – starts at 1, increases by 1
- n – nr of responses in campaign

$$\text{Percentage} = \frac{\text{Average score}}{\text{Questionnaire max score}} \times 100$$

Equation 4 Average score percentage per campaign

- Average score – the number obtain in Equation 3
 - Questionnaire max score – the maximum questionnaire score
- The **Close** button will be Visible **only** if campaign State is Active. Pressing close will:
 - Change the campaign state to Closed
 - The Close button will disappear
 - The campaign won't accept new answers – the link will be disabled.
 - The **Print** button – will print, in a pdf like form, all information presented in this form. All the information from this form will be printed one after the other.
- **Statistics**
- **On the right** we have the following buttons:
 - **View Responses** button – will open a pdf like view where the creator will be able to view all individual responses, please refer to 5.5.3 for details.
 - **Download data** – will download all data pertaining to a campaign in an excel file, please refer to 5.5.4 for details.
 - **On the left** we have the following statistics:

- **Maximum score:** The system will display the maximum score obtained per campaign. Warning this **is not** the questionnaire max score, this represents the maximum score obtained by users or user and will be calculated as presented in Equation 5, whereas the percentage is calculated in Equation 6. The maximum score of a questionnaire can be 1000 but from all the answers the maximum score obtained in campaign can be 850.

$$\text{Maximum score per campaign} = \text{MAX}(\text{Responses score per campaign})$$

Equation 5 Max score per campaign

- MAX – represents the MAX function which calculates the maximum value from a given set of values
- Responses score per campaign – all the responses scores per campaign, they will be used as input values for the MAX function.

$$\text{Percentage} = \frac{\text{Max score}}{\text{Questionnaire max score}} \times 100$$

Equation 6 Max score percentage per campaign

- Max score – the number calculated above, Equation 5
 - Questionnaire max score – the maximum questionnaire score
- **Minimum score:** The system will display the minimum score obtained per campaign, calculated as presented in Equation 7, whereas the percentage is calculated in Equation 8.

$$\text{Minimum score per campaign} = \text{MIN}(\text{Responses score per campaign})$$

Equation 7 Min score per campaign

- MIN – represents the MIN function which calculates the maximum value from a given set of values
- Responses score per campaign – all the responses scores per campaign, they will be used as input values for the MIN function.

$$\text{Percentage} = \frac{\text{Min score}}{\text{Questionnaire max score}} \times 100$$

Equation 8 Min score percentage per campaign

- Min score – the number calculated above, Equation 7

- Questionnaire max score – the maximum questionnaire score
- No of responses with a score over 70%: The system will display the number of responses and the percentage (e.g., 3(5%)). The value (over70) will be calculated following the algorithm described in Equation 9, whereas the percentage is detailed in Equation 10:

Initialize:

```

n – number of responses per campaign;
over70 = 0;
70score = questionnaire max score × 0.7
for i to n do
    if obtained score > 70score
        over70 ++;
    end if
end for

```

Equation 9 Pseudocode for number of responses over 70% per round

- *i* – starts at first response in the campaign
- *n* – represents the total number of responses per campaign
- *over70* – the variable that will count the no of responses over 70% per campaign
- *70score* – represents the value of 70% of the maximum questionnaire score and it's calculated as shown in the initialize part of the pseudocode in Equation 9.

$$\text{Percentage} = \frac{\text{over70}}{\text{No of responses per campaign}} \times 100$$

Equation 10 Percentage of responses over70 per campaign

- *over70* – this number is calculated in Equation 9
 - no of responses per campaign – no of responses in the campaign
- No of responses with score below 50%: The system will display the number of responses and the percentage (e.g., 3(5%)). The value (below50) will be calculated following the algorithm described in Equation 11, whereas the percentage is detailed in Equation 12:

Initialize:

```

    n – number of responses per campaign;
    below50 = 0;
    50score = questionnaire max score × 0.5
for i to n do
    if obtained score < 50score
        below50 + +;
    end if
end for

```

Equation 11 Pseudocode for number of responses below 50% per campaign

- i – starts at first response in the campaign
- n – represents the total number of responses per campaign
- below50 – the variable that will count the no of responses below 50% per campaign
- 50score – represents the value of 50% of the maximum questionnaire score and it's calculated as shown in the initialize part of the pseudocode in Equation 11.

$$\text{Percentage} = \frac{\text{below50}}{\text{No of responses per campaign}} \times 100$$

Equation 12 Percentage of responses below50 per campaign (relative to number of responses)

- Below50 – this number is calculated in Equation 11
 - no of responses per campaign – no of responses in the campaign
- No of questions where more than 50% of people obtained below 50%: The system will display the number of questions that fulfils the condition. The pseudocode for calculating the number is presented in Equation 13, the variable that will be displayed is named <NoOfCommonQuestionsPerCampaign>.
 - Questions where more than 50% of people obtained below 50%: The system will display the name of the questions that fulfils the condition. The pseudocode for displaying the names is presented in Equation 13, the variable that will be displayed is a vector type named <CommonQuestionsPeCampaign(vector)>.

Initialize:

```

n no of responses in campaign
k no of questions
Question (matrix)
CommonQuestionsPeCampaign(vector)

```



```

        NoOfCommonQuestionsPeCampaign
    for i to n
        for j to k
            if (question score < question max score × 0.5)
                Questioni,j = j
            end if
        end for
    end for
    CommonQuestionsPerCampaign = ∩ of all Question (matrix) rows
    NoOfCommonQuestionsPeCampaign = sizeof(CommonQuestionPerCampaign)

```

Equation 13 Pseudocode for all questions with score below 50% per campaign

- n – number of responses
- k – number of questions
- Question (matrix) – this matrix will store all the questions that fulfil the condition (the question individual score is less than 50% of the question max score). The algorithm will store on each row all the questions for every response. The matrix will have as many rows as total number of answers.
- CommonQuestionsPerCampaign (vector) – this vector will represent the intersection of all matrix rows trying to find common elements in all the rows. In order to optimise the algorithm this vector will be calculated as:
 - The algorithm will find the row in the Question (matrix) that has the least number of elements
 - This row will be compared with all other rows in the Question (matrix) in order to see which of those elements are common to all other rows in the matrix.
- NoOfCommonQuestionsPerCampaign – represents the sizeof CommonQuestions vector.

- Graphs

- Overall response score distribution
 - This graph will represent the overall response score distribution. The data used for this graph will be the response total score. Please refer to Figure 25 for details on graph look.
- Response score distribution per question
 - This graph will represent the evolution of the score distribution per each questionnaire question. The data used for this graph is each question score per response. Please refer to Figure 25 for details on graph look.

5.5.2. Design screen with data

In order to make explanations easier the following questionnaire design information will be used, Table 10.

Item	Description
Campaign name	Malware identification
Campaign description	Campaign about malware identification
Campaign state	Active
Questionnaire name	Malware questions
Questionnaire max score	1000
No of questions	10
No of responses	10
Campaign start date	Start date 5 Jan 2021 9:00 AM
Campaign end date	N/A
Q1 max score	100
Q2 max score	50
Q3 max score	50
Q4 max score	200
Q5 max score	50
Q6 max score	50
Q7 max score	150
Q8 max score	100
Q9 max score	100
Q10 max score	150

Table 10 Dummy campaign information

The dummy data for campaign responses is presented in Table 11.

Responses	Score Q1	Score Q2	Score Q3	Score Q4	Score Q5	Score Q6	Score Q7	Score Q8	Score Q9	Score Q10	Total score
Response1	50	20	50	100	50	50	100	70	70	100	660
Response2	100	50	50	200	50	50	150	100	100	120	970
Response3	50	20	50	50	50	50	100	50	50	50	520
Response4	100	20	20	200	20	50	70	100	100	150	830
Response5	50	20	20	50	20	20	70	50	50	70	420
Response6	70	50	50	100	50	50	100	70	70	100	710
Response7	100	50	50	200	50	20	150	100	100	150	970
Response8	100	20	50	200	50	50	100	50	50	50	720
Response9	100	20	20	200	50	50	70	100	100	150	860
Response10	50	20	20	50	20	20	50	50	50	50	380

Table 11 Dummy campaign response data

Campaign name:

Campaign description:

Campaign state: Active No of responses:

Campaign start date: Campaign end date:

Questionnaire in the campaign:

Questionnaire max score: No of questions:

[Close](#) [Print](#)



Statistics

Maximum score: [View Responses](#)

Minimum score: [Download data](#)

No of responses with score over 70%:

No of responses with score below 50%:

No of Questions where more than 50% of people obtained a score below 50%:

Questions where more than 50% of people obtained below 50%:

Graphs



Figure 25 Campaign statistics design screen with data

Below are some explanations for Figure 25. All data presented is **Read Only**. The data is the same as the one depicted previously in Figure 24, but this time the form is filled with the dummy data presented in Table 10 and Table 11. This explanation will concentrate on the formulas and the numbers obtained, as follows:

- The fields: Campaign Name, Campaign Description, Campaign state, Questionnaire in the campaign, Campaign End date, Questionnaire max score, no of responses, No of Questions - will be filled with the static data presented in Table 10.
- AverageScore – Field will be calculated based on formula presented in Equation 3 for value and Equation 4 for % using data from Table 11. The value obtained is 704(70.4%). The field will be formatted with green because the score is above 70%.
- **Statistics**
 - o **On the right** – there will be the **View Reponses** and **Download data** buttons that will behave as described above (section 5.5.1)
 - o **On the left** we have the following statistics:
 - **Maximum score:** The value and percentage are calculated using Equation 5 and Equation 6 respectively. For the dummy data used in this example the values are: 970 (97%).
 - **Minimum score:** The value and percentage are calculated using Equation 7 and Equation 8 respectively. For the dummy data used in this example the values are: 380 (38%).
 - **No of responses with score over 70%:** The value and percentage are calculated using Equation 9 and Equation 10 respectively. For the dummy data used in this example the values are: 6 (60%).
 - **No of responses with score below 50%:** The value and percentage are calculated using Equation 11 and Equation 12 respectively. For the dummy data used in this example the values are: 2 (20%). **Warning:** The two scores: “No of responses with score over 70%” and “No of responses with score below 50%” shouldn’t necessary sum up to 100% , if there are responses with scores between (50% and 70%), like in our example, the values will not sum up to 100%.
 - **No of questions where more than 50% of people obtained below 50%:** The system will display the number of questions that fulfils the condition. The pseudocode for calculating the number is presented in Equation 13, the variable that will be displayed is named <NoOf CommonQuestionsPerCampaign>. For our example the value is 1.
 - **Questions where more than 50% of people obtained below 50%:** The system will display the name of the questions that fulfils the condition. The pseudocode for displaying the names is presented in Equation 13, the variable that will be displayed is a vector type named <CommonQuestionsPerCampaign>. For our example the value is Q2 (meaning question 2).
- **Graphs**
 - o **Overall response score distribution**

Figure 26 details are described below:

- Individual security assessment **X** of **total** – this read only box will show the number of the current individual security assessment out of total number of questions. Each response will have an individual security assessment.
- Navigation bar (5 icons detailed in order from left to right):
 - o First assessment
 - o Previous assessment
 - o Current assessment – if the user fills in a number and presses enter that assessment will be shown
 - o Next assessment
 - o Last assessment
- Regarding the navigation bar the user will be able to move through assessments and select the assessment, skip some, and go back.
- **Back** button – Pressing back button will close this screen and will send the user back to the Campaign statistics screen Figure 25.
- Individual security assessment – this represents the assessment which will be loaded every time the users change the navigation. When the screen is first loaded the system will display the first assessment (for the first response). The Individual security assessment is read only and is the same one as depicted in 5.4.3.

5.5.4. [Download all data](#)

Pressing the Download all data button will generate an excel file that contains all the campaign data as presented in Table 10 and Table 11. The system will not include any statistics or sums (besides the total response score). The excel file will contain raw campaign and response data.

6. Questionnaire design and content

6.1. Introduction

As per requirements from the Grant Agreement, stated in Chapter 1.1, the content of the questionnaire will be developed taking into consideration the findings from WP2 and the requirements from WP3.

The questionnaire will not exceed 10 pages and will be structured around the following topics:

- use of cybersecurity defences
- organisational measures,
- cost-benefit considerations,
- awareness of fundamental rights such as the rights to privacy,
- protection of personal data and the free movement of persons.

After the questionnaire is agreed in the consortium it will be disseminated to SMEs and CSOs with the goal of obtaining at least **100 responses** until the end of the project. The respondents will fill-in the questionnaire anonymously and will receive a score and guidelines on how to improve their security posture.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

At the end of the project a report will be published containing both a quantitative and a qualitative analysis of responses.

6.2. Industry benchmarking: common attack vectors

In order to define the CC-DRIVER self-assessment questionnaire content the most common attack vectors should be identified. We have chosen the most well-known sources that publish attack vectors and the latest charts for 2021.

These sources are:

- Open Web Application Security Project (OWASP) top 10 [OWA21] – the leading entity in publishing the most used web attack vectors for computer compromise using available data on compromised systems. OWASP top 10 mentions the most common categories of web attacks that are used in compromising entities and represents the industry gold standard.
- SysAdmin, Audit, Network, and Security (SANS) top new attacks and threats [SAN21] is a report published by SANS on the new attacks and threats in 2021
- State of the Phish – an annual report published by Proofpoint detailing the methods used by attackers to compromise companies through phishing [PRF21]. This report refers exclusively to phishing and the form of doing phishing attacks. Thus, the most common way of perpetrating phishing attacks is email, there are new ways nowadays that work in conjunction with email, most of them used to bypass 2FA.
- Balbix report – a report on most common attack vectors and breach methods [BAL19]. These methods detail is straight forward with the exception of trust relationships. Trust relationships refers to a relation of trust between two components like servers which is abused, this can happen through a Man in the Middle (MiTM) attack, weak encryption etc.
- Verizon Data Breach Investigations Report (DBIR) – an investigation report by Verizon [VER21]
- Security score card – a blog post on Common cyber-attack vectors in 2021 [SSC21]
- Upguard – a blog post on the 16 most common attack vectors in 2021 [UPG21]
- Dig8ital – a post about the most common cyber-attacks vectors of 2021 [DIG21]
- Rapid7 – a post about Common Types of Cybersecurity Attacks [RAP21]

The sources mentioned above make their own classification of the attack vectors, many of them include attack vectors from the same category. Table 12 represents all the raw data from the above-mentioned sources grouped with web attack categories. Comments were included only where additional explanations are needed for understanding.

Attack vector	Source	Comments
A01:2021 – Broken Access Control	OWA21	The OWASP top 10 details technical attacks against applications. They represent the top 10 most used attack vectors and might change over time. These categories show the technical methods used, though for some, the initial attack vector
A02:2021 – Cryptographic Failures		
A03:2021 – Injection		

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

Attack vector	Source	Comments
A04:2021 – Insecure Design		might be some sort of social engineering. For example, A01 – Broken Access Control might start with a phishing email where the attacker tricks the user to give-up his credentials. After that the attacker will use the credentials to log-in into the application.
A05:2021 – Security Misconfiguration		
A06:2021 – Vulnerable and Outdated Components		
A07:2021 – Identification and Authentication Failures		
A08:2021 – Software and Data Integrity Failures		
A09:2021 – Security Logging and Monitoring Failures		
A10:2021 – Server-Side Request Forgery (SSRF)		
Highly targeted phishing campaigns	SAN21	SANS proposes a mix of social attacks (phishing, mobile), with pure technical attacks for the others. Mobile devices started to be attacked because of the 2FA codes used for authentication. Most mobile attacks consist in tricking the user to reset their own password by pressing the reset link on an unsolicited SMS or SIM swapping.
Finding vulnerabilities in software (including security products)		
Mobile device attacks		
Persistent and Promiscuous Web Agents		
Email attacks	PRF21	The state of the phish report contains only social attacks that refer to how phishing campaigns are being disseminated.
Social media attacks		
Smishing attacks		
Vishing attacks		
USB drops		
Compromised credentials	BAL19	The Balbix report details the most common technical attack vectors, which can be divided into the same categories identified by OWASP.
Weak and stolen credentials		
Malicious insiders		
Missing or poor encryption		
Misconfiguration		
Ransomware		
Phishing		
Trust relationships		

Attack vector	Source	Comments		
Zero-day vulnerabilities				
Brute force attacks				
DDoS				
Denial of Service (DDoS and DDoS)	VER21	Verizon lists the most prevalent technical attacks and separately social engineering.		
Lost and stolen assets				
Miscellaneous errors				
Privilege misuse				
Social engineering				
System intrusion				
Basic web application attacks				
Everything else				
Phishing			SSC21	This report lists, besides the most common application attack vectors, malicious insiders and remote workforce. These two things can help an attacker succeed with the common attack vectors. A malicious insider might install malware himself or use inside information to create a very credible phishing campaign. The remote workforce is more susceptible to phishing campaigns and needs more training.
Malware				
Ransomware				
Denial of Service (DDoS) Attacks				
Compromised Credentials				
Malicious Insiders				
Misconfiguration				
A Lack of Encryption				
Web Application Attacks				
Your Remote Workforce				
Compromised Credentials	UPG21	The Upguard post details the most common technical attack vectors, which can be divided into the same categories identified by OWASP.		
Weak Credentials				
Malicious Insiders				
Missing or Poor Encryption				
Misconfiguration				
Ransomware				

Attack vector	Source	Comments
Phishing		
Vulnerabilities		
Brute Force		
Distributed Denial of Service (DDoS)		
SQL Injections		
Trojans		
Cross-Site Scripting (XSS)		
Session Hijacking		
Man-in-the-Middle Attacks		
Third and Fourth-Party Vendors		
Supply chain compromise	DIG21	Dig8ital blog post lists one the hardest to catch methods of attack supply chain compromise. This is a method that compromised the supply chain of the intended target using common technical attack vectors.
Malware		
Ransomware		
Phishing		
Threats from within		
Malware	RAP21	The Rapid7 post details the most common technical attack vectors, which can be divided into the same categories identified by OWASP.
Phishing		
SQL Injection Attack		
Cross-Site Scripting (XSS)		
Denial of Service (DoS)		
Session Hijacking and Man-in-the-Middle Attacks		
Credential Reuse		

Table 12 Attack vectors raw data

From Table 12 we can see that many sources identified the same attack vectors, but some included: processes, attacker types, and technical vectors. The first thing we must do is to try to classify the findings. To this effect we'll use our previous work we have done in this project.

Deliverable D.2.1 Nature of and perspectives on cybercrime explores the cybercrime phenomenon. The report details the following topics:

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Defines working definitions on cybercrime,
- Details how various EU states incorporated legal definitions into their legislation regarding cybercrime,
- Explores the extent of the cybercrime phenomenon including cybercrime as a service
- Provides characteristics of the offenders and victims and details the modus operandi of the attackers.

Tables 10, 11 and 12 from the aforementioned report (D2.1) synthesises the most prominent cyberthreats from the law enforcement point of view.

Type	Methods	Comments
Cyber-dependant crime	Business Compromise (BEC)/ Email Account Compromise (EAC)	Cyber-dependant crime
Child sexual exploitation online	Live streaming	Increase of the amount of online child sexual abuse material detected.
Payment fraud	SIM swapping Smishing Business email compromise Online investment frauds Card not present fraud Cryptojacking	These trends increased during COVID 19 because of the surge in online shopping even for basic products such as food items.

Table 13 Deliverable D2.1- results synthesis

Deliverable D3.1 Report on drivers of cyber juvenile delinquency presents a review of cyber adult and juvenile criminality and identifies the human factors and key drivers for cyber-criminality. Additionally, the report includes the finding from interviews conducted with: with 18 experts, 7 academics (from a range of disciplines) and 11 LEAs (36 in total), working in the field of juvenile cyber-criminality and delinquency.

Though deliverable D3.1 contains a lot of classification from existing literature, summarises the findings from the expert interviews which represent a very good picture for drivers for cyber-crime for both adults and youth.

The results of our research with cybercrime experts will inform the development of evidence-based educational, awareness and intervention tools and programmes in CC-DRIVER, for instance, a "pathways into cybercrime" checklist (PCC) resource for parents, caregivers and educators designed to help recognise youth behaviours that may facilitate cybercriminality and

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

a youth self-assessment metric (YSM) designed to assess the vulnerability of young people to cybercrime and to divert youth from cybercrime into more socially beneficial contributions.

Eleven themes emerged that were grouped under four overarching categories as follows:

- cybercrime prevention;
- pathways into cybercrime;
- motivations;
- and intervention methods.

Findings highlighted that tailored education and awareness raising are crucial to the prevention and tackling of juvenile cybercrime. The interview analysis shed light on the significance of social contexts, teenage curiosity and experimental interest in cyberspace, unmonitored accessibility to the world wide web, and device usage when considering juvenile cybercrime and risky actions online. Additionally, there is a need to support young people who have a curiosity for technology and cyberspace into developing their skills legally, using like-minded tech-skilled mentors.

There were several calls for ‘good practice’ guidelines to combat cybercrime among young people. A comprehensive set of practices is currently unaccounted for and is required for key stakeholders to be well-equipped to detect, deter and divert young people from committing dangerous activities online. As offences transcend international borders, there is an increasing demand to clarify legal frameworks, rules and regulations. Modernised laws on an international scale were recommended to clarify the response these key actors can implement in the shifting technological landscape.

There was a perceived dual responsibility to safeguard victims and implement effective strategies to protect vulnerable children and young people. On a psychological and pathological level, appropriate support and protection needs to be available for victims that are direct recipients of an online offense, and indirectly for individuals that misuse the Internet putting themselves at a risk of self-harm. To safeguard young people, cyber victimisation emerged as a critical consideration through access to supportive materials and advice, increased digital censorship of harmful material and effective online protection strategies to be implemented.

Overall, respondents were keen not to blame and punish young people who may have engaged in cybercrime, but rather to raise awareness of what is or isn't a crime online, and to support vulnerable young people to make better informed choices. Broadly, findings are reflective of current literature, but also offer new and un-explored concepts, particularly as this study was conducted in the context of cybercrime perpetration during COVID-19, and the new emerging cybercrime trends the pandemic has highlighted.

Considering how vast the classifications are from different sources we are going to use the following classifications to propose best practices:

- **People:**
 - Cyber criminals (external attackers) – these are the external cyber criminals that what to do harm to a company. The company they target might be the indented target or just a step for them to get to their final goal (supply chain attacks). Cyber criminals can use everything from launching phishing campaigns to doing technical attacks themselves.

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- Malicious insiders – malicious insiders are cybercriminals who work or worked for the company and have intimate knowledge of the company’s systems. They are the most dangerous threat because they can install malicious software themselves or delete important data.
- Unintentional breaches – mostly these are performed unintentionally by good employees that are unaware of what they do. These can be losing a company device, re-use the same credentials, click on a phishing link, not running computer updates on time, not changing default passwords on personal devices such as home routers, security misconfigurations of company devices.
- **Damage to organisation business environment:**
 - Attacks on the organisational procedures and supply chain – organisations must have in place procedures to vet their suppliers and to make sure they maintain minimum security standards. Also, their own security procedures must be updated at least once a year.
 - Technological failures / natural disasters and infrastructure damage – technology can fail but itself in a natural disaster where the servers are physically destroyed or it can be helped by an attacker through DDoS, ransomware, malware.
 - Technical attacks – all technical attacks that were mentioned in OWASP top 10 and others are included in this category.

6.3. Industry benchmarking: best practices

There are many proposals for security controls that should be implemented in an organisation, but two sources are often most cited: SANS CIS Controls (Critical Information Security) v8 [CIS21] and National Institute of Standards and Technology (NIST) SP 800-53 [NIST21]. The problem with all of these controls is that they can’t be implemented in their entirety by SMEs due to lack of security budget, which translated in the lack of security tools and in-house security personnel. In most cases the system administrator of a SME is also the “security person”.

According to Microsoft [MIC19] there is one thing a company can do to prevent 99,99% of attacks and that is to implement MFA (multi factor authentication), considering that there are over 300 million fraudulent sign-in attempts on cloud service every day.

The most important resource for an organisation is the human resource, which can also be its greatest weakness. This is why a security awareness program is very important for any organisation and can prevent up to 90% of malicious data breaches.

Table 14 represents a summary of all attacks vectors and security measures presented in this chapter, which will be used to create the SMEs questionnaire that will assess their security exposure to cyber-crime. The security measures were classified using the requirements stated in GA, some measure can be classified in more than one category:

- use of cybersecurity defences (1)
- organisational measures (2)
- cost-benefit considerations (3)
- awareness of fundamental rights such as the right to privacy (4)
- protection of personal data and the free movement of persons (5)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

Attack vector	Security initiatives / Category
Social engineering (phishing, vishing, USB drops, malware installation, credential divulcation, smishing)	Security awareness programs (2)
Broken Access Control (Compromised credentials, Weak or stolen credentials, Credential Reuse, Brute force)	Security awareness programs (2) Least privilege access (1,2) No anonymous accounts (1,2) Rotate passwords (1,2) Least privilege access (1,2) Remove access rights (1,2) Password manger implementation (1,2,3)
Identification and Authentication Failures	Monitoring and alerting on multiple log-in failures from the same accounts (1,2) Monitoring and alerting on log-in from different locations (1,2) Emergency access removal procedure (2)
Business email compromise	Implement MFA for critical accounts (1, 2, 3, 4, 5)
Cryptographic Failures (Missing encryption, poorly configured encryption)	Implement known and up to date cryptographic protocols (1) Use encryption all over - no mixed content (1, 2, 4, 5)
Zero days vulnerabilities	Network segregation (1, 2) Monitor logs (1) Monitor and alert on privilege escalation (1, 2, 3, 4, 5)
Known vulnerabilities (Vulnerable and Outdated Components)	Regular updates of devices and software - OS and applications (1, 2) Run automatic vulnerability scans (1, 2)
Malware including Persistent and Promiscuous Web Agents	Business continuity and data recovery (1, 2, 3, 4, 5) Cyber insurance (3)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

Attack vector	Security initiatives / Category
	Regular updates of devices and software OS and applications (1, 2)
Security Misconfiguration and insecure design	Fail in a secure state (1) Run automatic security vulnerability scans (1)
Malicious insiders	Network segregation (1, 2) No anonymous accounts (1, 2) Least privilege access (1,2) Remove access rights (1,2) Automatic alerts on accessing unauthorised resources (1, 2)
Lost or stolen assets	Updated list of all hardware, software and access points (1, 2, 4, 5) Remote device wiping (1) Device encryption (1, 2)
Miscellaneous errors	Fail in a secure state (2) Security by design (1)
Supply chain compromise (Third and Fourth-Party Vendors)	Use vendors with adequate security (at least ISO 21000) Annual review of vendor security audit reports Monitor vendors List of all vendors and assets
Software and Data Integrity Failures	Trust but verify (1,2) Input sanitization (1,2) Encrypted communication (1, 2)
Security Logging and Monitoring Failures	Automatic alerts for most important incidents (1,2)
Mobile device attacks	Updated list of all hardware, software and access points (1, 2, 4, 5) Remote device wiping (1) Device encryption (1, 2)
Other web application attacks: Session Hijacking and Man-in-the-Middle Attacks,	Use of WAF (1)

Attack vector	Security initiatives / Category
SQL Injections, Server-Side Request Forgery (SSRF), Cross-Site Scripting (XSS), Denial of Service (DDoS and DDoS), Man-in-the-Middle Attacks etc	Use of parametrised statements (1) Update all software and hardware (1, 2) Input sanitization (1) Use of CDN - Content Delivery Network (1) Use encryption (1) Use of automatic application security frameworks (1) Penetration tests and vulnerability scans (1,2)
Data protection (employees and customer)	Access control (1,2) Least privileged access (1,2) Monitor and alert on privilege escalation (1, 2, 3, 4, 5) Monitor and alert on successive failed log-in attempts from the same account (1,2) Data and device encryption (1, 2)

Table 14 Vulnerability assessment test areas

Most experts and our own research conducted in WP3 conclude that the most important factors that allow the success of cyber criminals are human factors. These factors are classified best into:

- **Human factors – do something that will result in a security incident.** In this category we have phishing that requires a human to click a link and install malicious software by mistake
- **Human error or complacency in relation to cyber security** – not doing something that will result in a security incident. In this category we have scan and exploit–hackers will scan everything, so if a system admin forgets to change the default admin password before making the web servers accessible from the internet that server is compromised
- **Both categories** – we have **unauthorised use of credentials** like:
 - shoulder surfing – credentials are stolen when someone is introducing them and it's not attentive about his environment
 - phishing - tricking a person into entering login credentials into a spoof login page
 - social engineering - tricking a person into handing over a login credential over the phone, social media, or using other communication methods, such as emails, help desks and texts

We have proposed a number of 45 questions grouped in the afore mentioned categories. Some questions can be included in more than one category. The division of questions per each category is as depicted in Table 15:

Classification	Types	Number of questions
DoA classification	Use of cybersecurity defences	38
	Organisational measures	21
	Cost-benefit considerations	10
	Awareness of fundamental rights such as the right to privacy	12
	Protection of personal data and the free movement of persons	12
Human drivers for cyber criminality	Human factors	16
	Human error	43

Table 15 Classification of the questions

We want to mention the following regarding the questions and questionnaire:

- One answer is expected form each question.
- Each question has a maximum score that can be obtained.
- The user will receive a score based on the choice he/she makes.
- Sometimes two choices will have the same score, which means both situations are acceptable in practice.
- The questions are not weighted, but they have a different maximum score.
- The maximum score of a question was set up based on the most prevalent attack vectors described above.

Table 15 depicts the classification of the questions into the aforementioned categories:

Question number	Question	Categories*						
		1	2	3	4	5	6	7
1.	The Information security policy document represents a set of rules and guidelines who work with IT assets. How detailed is your information security policy?		x				x	x

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

Question number	Question	Categories*						
		1	2	3	4	5	6	7
2.	A security awareness session is a training to makes employees aware of security procedures that are in place in the organisation. Do you provide regular security awareness training in your organisation?		X				X	X
3.	Phishing is a form of cyber-attack usually by email which aims to trick the user into installing malware or following a link and providing personal information. Do you provide separate training regarding phishing		X				X	X
4.	Did you analyse and create a remote working policy and other specific policies as response to COVID-19?		X				X	X
5.	Does your password policy specify the minimum password length?	X	X				X	
6.	Does your password policy specify the mandatory password composition from each category? (The categories are: small caps, large caps, symbols, and numbers)	X	X				X	
7.	What is the best practice mentioned in your security policy regarding using passwords for multiple accounts?	X	X					X
8.	Do you have firewalls between your organisation's internal networks and the internet?	X	X					X
9.	When you first receive a device (router or any hardware) or administrator accounts for applications do you change the default password?	X	X					X
10.	How do you ensure that you know to change passwords after they have been compromised?	X	X					X

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

Question number	Question	Categories*						
		1	2	3	4	5	6	7
11.	Do you have an emergency access revoke or account suspension procedure?	x	x					x
12.	Do you have formal logging for all your digital assets and services your company has?	x	x					x
13.	Do you have any services enabled that are accessible externally from your internet routers or hardware firewall?	x						x
14.	Have you configured your internet routers or hardware firewall devices so that they block all other services from being advertised to the internet?	x						x
15.	Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet?	x						x
16.	Do you have software firewalls enabled on all of your computers and laptops?	x						x
17.	Have you disabled 'auto-run' or 'auto-play' disabled on all of your systems?	x						x
18.	How do you ensure patching of all known vulnerabilities in the software and hardware (firmware) you use?	x						x
19.	Do you update high-risk security updates for OS and applications within 14 days of release?	x						x
20.	Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password?	x						x

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

Question number	Question	Categories*						
		1	2	3	4	5	6	7
21.	Do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?	x						x
22.	Do you ensure that staff members only have the privileges that they need to do their current job? How do you ensure long term employees don't accumulate access rights?	x						x
23.	Do you have a formal process for giving someone access to systems at an "administrator" level?	x						x
24.	Do you formally track which users have administrator accounts in your organisation?	x						x
25.	Do you ensure that administrator accounts are not used for accessing servers other computers, email, browsing etc?	x						x
26.	Do you review who should have administrative access on a regular basis?	x						x
27.	Have you enabled two-factor authentication for access to administrative accounts?	x						x
28.	Do you have automatic notifications when an account has had 5 or less incorrect log-in attempts?	x						x
29.	Do you have automatic notifications when an user logs-in from a different location then the one he usually does? (example: he usually logs-in in from US and now suddenly logs-in from China).	x						x
30.	Do you have automatic notifications and monitoring for privilege escalation	x						x

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

Question number	Question	Categories*						
		1	2	3	4	5	6	7
	(example: when a command is run with “sudo” or administrative account)?							
31.	Do you use encryption in your company?	x	x	x	x	x	x	x
32.	Network segregation is the separation of critical networks from the Internet and other internal, less sensitive networks. A zero day vulnerability is a vulnerability unknown to the producer of a software application or hardware device. Let's assume a hacker uses a zero day vulnerability to hack your company. What are the most important security controls that you have set-up to stop the advancement of that intruder?	x	x	x	x	x	x	x
33.	Are all of your computers, laptops, tablets and mobile phones protected from malware?	x		x	x	x	x	x
34.	Do you have backups of all your server's data (business critical data)?	x	x	x	x	x	x	x
35.	Where do you store backups?	x	x	x	x	x	x	x
36.	Have you run a full backup restore exercise?	x	x	x	x	x	x	x
37.	Do you run automatic vulnerability scans?	x	x	x	x	x	x	x
38.	Do you have a list with all your vendors that supply OS and applications?		x	x	x	x	x	x
39.	Do you do a comprehensive security audit of these vendors?		x	x	x	x	x	x
40.	Do you have signed SLAs Service Level Agreements (SLAs) with vendors that supply your business with critical components including liability?		x	x			x	x

Question number	Question	Categories*						
		1	2	3	4	5	6	7
41.	Do you regularly perform scans to identify unauthorized or rogue wireless access points?	x						x
42.	Have you deployed IDS (Intrusion Detection System) on the wireless network of your organisation?	x						x
43.	What type of encryption do you apply for the protection of the WiFi - SSID password, thus authentication and transmission over wireless network?	x			x	x		x
44.	Have you implemented or deployed a DLP (Data Loss Prevention) system?	x			x	x		x
45.	Have you deployed a honeypot system on your internal network as a proactive measure to detect an intruder?	x			x	x		x

* The following notation for categories was used:

1. Use of cybersecurity defences
2. Organisational measures
3. Cost-benefit considerations
4. Awareness of fundamental rights such as the right to privacy
5. Protection of personal data and the free movement of persons
6. Human factors
7. Human error

The proposed questionnaire with questions and options can be found in Annex 2 – Vulnerability self-assessment questionnaire.

7. Conclusion

This document detailed the functionalities of the vulnerability Self-Assessment Questionnaire (SAQ) application, that allows the design of questionnaires using the graphical interface. The document details all the application functionalities and flows.

This document contains the Vulnerability Assessment questionnaire that will be sent to SMEs and CSOs to help them assess their vulnerability in the following areas: cybersecurity defences,

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

organisational measures, cost-benefit considerations, awareness of fundamental rights such as the rights to privacy, protection of personal data and the free movement of persons.

We have designed 45 questions for the self-assessment questionnaire that will be used to determine the exposure of a SME, CSO to cyber criminality. The questions are divided into various categories such as: Use of cybersecurity defences, Organisational measures, Cost-benefit considerations, Awareness of fundamental rights such as the right to privacy, Protection of personal data and the free movement of persons, Human factors, Human error.

DRAFT

Annex 1 – Correspondence matrix

The following is a correspondence matrix from the requirements stated in the grant agreement and the ones defined in the application functionalities.

Requirement form Grant agreement	FR or NFR no
Co-develop and demonstrate a cybercrime vulnerability self-assessment questionnaire for SMEs and CSOs	FR1, FR2, FR3, FR4, FR5, FR6, FR7, FR8, FR9, NFR1, NFR2, NFR3, NFR4, NFR5, NFR6
Develop the online questionnaires taking into account the research findings from WP2 and the requirements from WP3.	FR1, FR2, FR3, FR4, FR5, FR6, FR7, FR8, FR9, NFR1, NFR2, NFR3, NFR4, NFR5, NFR6
The user will be able to complete the questionnaire in an anonymous way.	FR6
They will receive a score and afterwards guidelines on the countermeasures that they can undertake against the vulnerabilities.	FR7
Stakeholders will be able to download the self-assessment questionnaire or complete it anonymously via the EU survey website.	FR9
The scoring of each user will derive from which of the five responses users tick to each question.	FR4, FR6, FR7
CC-DRIVER will first develop a questionnaire suitable for SMEs and CSOs across Europe. The questionnaire will not be more than 10 pages and will be structured according to different types of questions -- use of cybersecurity defences, organisational measures, cost-benefit considerations, awareness of fundamental rights such as the rights to privacy, protection of personal data and the free movement of persons.	NFR5
KPI: Dissemination of the online cybercrime vulnerability self-assessment tool to national SME associations by M20 with 100 responses from SMEs and CSOs to the online self-assessment questionnaire before the end of the project	NFR6
An online vulnerability self- assessment questionnaire (R.8) - SMEs, CSOs, SMEs and CSOs will be able to use the tool anonymously online.	FR6, NFR6

Table 16 Correspondence matrix

Annex 2 – Vulnerability self-assessment questionnaire

Vulnerability Assessment questionnaire

One answer is expected form each question.

Each question has a maximum score that can be obtained. The user will receive a score based on the choice he/she makes. Sometimes two choices will have the same score, which means both situations are acceptable in practice.

- 1) The Information security policy document represents a set of rules and guidelines who work with IT assets. How detailed is your information security policy? (Max: 300)
 - a) Our security policy is detailed, sets the objectives, it's updated at least once a year and formally communicated to all employees (300)
 - b) Our security policy is detailed, sets the objectives, it's updated at least once a year (200)
 - c) Our organisation has an information security policy, but is not updated once a year (100)
 - d) Our organisation doesn't have a formal security policy (0)
- 2) A security awareness session is a training to makes employees aware of security procedures that are in place in the organisation. Do you provide regular security awareness training in your organisation? (Max: 100)
 - a) Yes, the security awareness training is mandatory for all employees and done every year after they join the company (100)
 - b) Yes, the security awareness training is mandatory for all employees and done every two or three years after they join the company (75)
 - c) Yes, the security awareness training is mandatory for all employees only when they join the company (50)
 - d) No, we do not provide a mandatory security awareness training (0)
- 3) Phishing is a form of cyber-attack usually by email which aims to trick the user into installing malware or following a link and providing personal information. Do you provide separate training regarding phishing? (Max: 200)
 - a) Yes, we provide separate phishing training and we have a phishing platform installed that runs campaigns several times a year (200)
 - b) Yes, we provide separate phishing training but we have no other measures in place (100)
 - c) No, we include information about phishing in the security awareness training (50)
 - d) No, we do not provide any phishing training (0)
- 4) Did you analyse and create a remote working policy and other specific policies as response to COVID-19? (300)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- a) Yes, we defined policies (like remote working policy etc) and trained all employees regarding the content of the policies and what to do when working from home (300)
 - b) Yes, we defined policies (like remote working policy etc) and sent them to employees to read and acknowledge it using a proper acknowledgement system (200)
 - c) Yes, we defined policies (like remote working policy etc) and send a companywide email with the policies (100)
 - d) No special policies were defined (0)
- 5) Does your password policy specify the minimum password length? (Max: 200)
- a) Yes, the password should be a 20 characters passphrase (200)
 - b) Yes, the passwords should be at least 10 characters (150)
 - c) Yes, the passwords should be at least 8 characters (100)
 - d) Yes, the password should be less than 8 characters (50)
 - e) No, our policy doesn't specify password length (0)
- 6) Does your password policy specify the mandatory password composition from each category? (The categories are: small caps, large caps, symbols, and numbers) (Max: 100)
- a) Yes, the password must contain at least one element from all four categories (100)
 - b) Yes, the password must contain at least one element from three categories (75)
 - c) Yes, the password must contain at least one element from two categories (50)
 - d) No, our policy doesn't specify anything about password composition (0)
- 7) What is the best practice mentioned in your security policy regarding using passwords for multiple accounts? (Max: 200)
- a) Our policy specifies that the user must have a unique and different password for each account, to aid with that we provide a password manager that all our employees have to use (200)
 - b) Users are advised to use different passwords for different accounts, but we do not provide a password manager (100)
 - c) Use one password for personal accounts and one for corporate accounts (0)
 - d) Use one password for all the accounts they own (0)
 - e) No advice regarding the use of passwords for multiple accounts is offered (0)
- 8) Do you have firewalls between your organisation's internal networks and the internet? (Max: 100)
- a) Yes (100)
 - b) No (0)
- 9) When you first receive a device (router or any hardware) or administrator accounts for applications do you change the default password? (Max: 200)
- a) Yes (200)
 - b) No (0)
- 10) How do you ensure that you know to change passwords after they have been compromised? (Max: 300)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- a) We have automatic dark web monitoring for our business emails and change all the accounts passwords that have been compromised (300)
 - b) We have a mandatory password reset every 90 days (300)
 - c) We have a mandatory password reset at least once a year (200)
 - d) We have a mandatory password reset exceeding one year (100)
 - e) We don't have automatic password reset nor monitoring for compromised accounts (0)
- 11) Do you have an emergency access revoke or account suspension procedure? (Max: 300)
- a) Yes (300)
 - b) No (0)
- 12) Do you have formal logging for all your digital assets and services your company has? (Max: 200)
- a) Yes, we use a specialised system to track those assets and every asset needs to be enrolled in the system before being used (200)
 - b) Yes, we use an excel sheet to keep a record of our assets and we manually add/remove assets (100)
 - c) We have a vague idea, but it's not enforced in a formal procedure (50)
 - d) No, we don't keep a record of all our digital assets (0)
- 13) Do you have any services enabled that are accessible externally from your internet routers or hardware firewall? (Max: 100)
- a) Yes, but all of them have a documented business case (100)
 - b) Yes, but the need is not documented (0)
 - c) No, our services are not accessible from the internet (100)
- 14) Have you configured your internet routers or hardware firewall devices so that they block all other services from being advertised to the internet? (Max: 100)
- a) Yes (100)
 - b) No (0)
- 15) Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet? (Max: 200)
- a) Yes, but we use 2FA (2 Factor Authentication) to log-in (200)
 - b) Yes, we use simple authentication username and password (100)
 - c) No, they don't provide access to configuration settings over the internet (200)
- 16) Do you have software firewalls enabled on all of your computers and laptops? (Max: 100)
- a) Yes (100)
 - b) No (0)
- 17) Have you disabled 'auto-run' or 'auto-play' disabled on all of your systems? (Max: 100)
- a) Yes (100)
 - b) No (0)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- 18) How do you ensure patching of all known vulnerabilities in the software and hardware (firmware) you use? (Max: 400)
- We run regular patch updates and all of our applications and Operation Systems (OSs) are supported by the manufacturer that provides regular patches (400)
 - We run regular patch updates on the applications and OS systems that allow it (we do have some End-of-Life applications and OS like Windows XP and Vista) (200)
 - We don't run regular updates (0)
- 19) Do you update high-risk security updates for OS and applications within 14 days of release? (Max: 400)
- Yes, for all our applications and OS (400)
 - Yes, for high-risk applications (200)
 - No, we don't run security updates within 14 days of release (0)
- 20) Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password? (Max: 300)
- Yes, we don't use shared computers (300)
 - Individual computers use unique accounts, but we use shared computers for administrative purposes (150)
 - No, we don't have individual accounts for laptops and servers (0)
- 21) Do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation? (Max: 250)
- Yes, we have a procedure for access removal when the employee leaves and we also do at least one annual check (250)
 - Yes, we have a procedure for access removal when the employee leaves and we also do some checks, though no time frame is set for this check and they don't happen regularly (200)
 - Yes, we have a procedure for access removal when the employee leaves (150)
 - Sometimes we delete or disable accounts, but it's not a defined process so this activity is not done regularly (50)
 - No, we don't have any process in place, and we don't usually do this activity (0)
- 22) Do you ensure that staff members only have the privileges that they need to do their current job? How do you ensure long term employees don't accumulate access rights? (Max: 200)
- Yes, we employ the least privilege principle and we do quarterly privileges access checks (200)
 - Yes, we employ the least privilege principle and we do privilege access checks (though we don't have a set time interval) (150)
 - Yes, we employ the least privilege principle but we don't do privilege access checks (100)
 - No, we do not have a process to check for access removal (0)
- 23) Do you have a formal process for giving someone access to systems at an "administrator" level? (Max: 200)
- Yes (200)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- b) No (0)
- 24) Do you formally track which users have administrator accounts in your organisation? (Max: 200)
- a) Yes (200)
 - b) No (0)
- 25) Do you ensure that administrator accounts are not used for accessing servers other computers, email, browsing etc? (Max: 200)
- a) Yes (200)
 - b) No (0)
- 26) Do you review who should have administrative access on a regular basis? (Max: 300)
- a) Yes, every 3 months (300)
 - b) Yes, every 6 months (200)
 - c) Yes, once a year (100)
 - d) Yes, more than a year (no defined interval) (50)
 - e) No (0)
- 27) Have you enabled two-factor authentication for access to administrative accounts? (Max: 300)
- a) Yes, for all (300)
 - b) Yes, for the critical ones (150)
 - c) No (0)
- 28) Do you have automatic notifications when an account has had 5 or less incorrect log-in attempts? (Max: 200)
- a) Yes, for all users (200)
 - b) Yes, for administrative accounts (100)
 - c) No (0)
- 29) Do you have automatic notifications when a user logs-in from a different location then the one he usually does? (Example: he usually logs-in in from US and now suddenly logs-in from China) (Max: 200)
- a) Yes, for all users (200)
 - b) Yes, for administrative accounts (100)
 - c) No (0)
- 30) Do you have automatic notifications and monitoring for privilege escalation (example: when a command is run with “sudo” or administrative account)? (Max: 200)
- a) Yes, we monitor all commands issued with administrative privileges (200)
 - b) Yes, only for business-critical servers (100)
 - c) No (0)
- 31) Do you use encryption in your company? (Max: 300)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- a) Yes, for everything: devices are encrypted, data storage is encrypted, and our communication is encrypted (300)
 - b) Yes, we encrypt our devices and our applications have standard encryption, but we don't do additional configurations (200)
 - c) No, we use default applications and we don't specifically activate device encryption (100)
- 32) Network segregation is the separation of critical networks from the Internet and other internal, less sensitive networks. A zero-day vulnerability is a vulnerability unknown to the producer of a software application or hardware device. Let's assume a hacker uses a zero-day vulnerability to hack your company. What are the most important security controls that you have set-up to stop the advancement of that intruder? (Max: 200)
- a) Network segregation and privilege escalation alerting (200)
 - b) Network segregation (100)
 - c) Privilege escalation alerting (100)
 - d) We don't have any specific controls configured (0)
- 33) Are all of your computers, laptops, tablets and mobile phones protected from malware? (Max: 250)
- a) Yes, we're using anti-malware software and we have enabled trusted sources (APP store or a list of approved applications) that our employees are allowed to install (250)
 - b) Yes, we're using anti-malware software (100)
 - c) No, we don't have anti-malware applications (0)
- 34) Do you have backups of all your server's data (business critical data)? (Max: 400)
- a) Yes, we have a very detailed procedure that includes full backups, incremental backups and clear SLA with stated RTO - Recovery Time Objective and RPO - Recovery Point objective (400)
 - b) Yes, we have scheduled a backup, but no clear SLA (200)
 - c) No, we don't have any backups for servers (0)
- 35) Where do you store backups? (Max: 400)
- a) Backups are stored on a specialised backup system that is segregated by the rest of the network (400)
 - b) Backups are stored on the same server or on another server, but the network is not segregated (200)
 - c) We don't have a clear location for storing backups or we don't store backups (0)
- 36) Have you run a full backup restore exercise? (Max: 300)
- a) Yes regularly (we have a scheduled exercise at least once a year) (300)
 - b) Yes, some time ago, but we don't have a regular activity (150)
 - c) No, we have never run a full backup restore (0)
- 37) Do you run automatic vulnerability scans? (Max: 300)
- a) Yes, every quarter (300)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

- b) Yes, every 6 months (200)
 - c) Yes, annually (100)
 - d) Yes, more than once a year, no interval defined (50)
 - e) No (0)
- 38) Do you have a list with all your vendors that supply OS and applications? (Max: 200)
- a) Yes, we have a comprehensive list of all our vendors and applications (internal and external) (200)
 - b) Yes, we have a partial list comprising of vendors for business-critical applications (100)
 - c) No, we don't have a list (0)
- 39) Do you do a comprehensive security audit of these vendors? (Max: 200)
- a) Yes, our internal security team checks every possible vendor before becoming a supplier and we also do annual security reviews of all our vendors (200)
 - b) Yes, we do a security check for business-critical vendors and an annual security review for them (150)
 - c) Yes, we do an initial check for vendors for business-critical processes, but we don't review it after that (100)
 - d) No, we have no procedure in place for doing vendor security review (0)
- 40) Do you have signed Service Level Agreements (SLAs) with vendors that supply your business with critical components including liability? (Max: 200)
- a) Yes, we have clear SLAs including liability, operating hours, service delivery terms etc (200)
 - b) No, we don't have SLAs in place (0)
- 41) Do you regularly perform scans to identify unauthorized or rogue wireless access points? (200)
- a) Yes, we do in a quarterly basis (200)
 - b) Yes, we do once in a year, approximately (100)
 - c) No, we never do (0)
- 42) Have you deployed IDS (Intrusion Detection System) on the wireless network of your organisation? (200)
- a) Yes, we have (200)
 - b) No, we haven't (0)
- 43) What type of encryption do you apply for the protection of the Wi-Fi - SSID password, thus authentication and transmission over wireless network? (200)
- a) WPA3-Enterprise (192-bit encryption) (200)
 - b) WPA3-Personal (128-bit encryption) (150)
 - c) WPA2-PSK (100)
 - d) WPA or WEP (50)
 - e) Our Wi-Fi is not password protected (0)

D4.2 [Cybercrime vulnerability self-assessment questionnaire]

44) Have you implemented or deployed a DLP (Data Loss Prevention) system? (100)

- a) Yes, we have (100)
- b) No, we haven't (0)

45) Have you deployed a honeypot system on your internal network as a proactive measure to detect an intruder? (100)

- a) Yes, we have (100)
- b) No, we haven't (0)

DRAFT

References

- [BAL19]** Balbix, Most Common Cybersecurity Attack Vectors and Breach Methods, https://www.balbix.com/app/uploads/eBook_Most-Common-Attack-Vectors-and-Breach-Methods.pdf
- [CIS21]** SANS, CIS controls v8, <https://www.sans.org/blog/cis-controls-v8/>
- [DIG21]** Dig8igital, The most common cyber-attacks vectors of 2021, <https://dig8ital.com/resources/library/the-most-common-cyber-attack-vectors-of-2021>
- [IEE98]** IEEE Standard 1233-1998, IEEE Guide for Developing System Requirements Specifications
- [IEE18]** IEEE 29148 - 2018 - ISO/IEC/IEEE International Standard - Systems and software engineering - Life cycle processes - Requirements engineering
- [ISO19]** ISO/IEC 27701:2019(en) Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- [MAT11]** Matt Walker. 2011. CEH Certified Ethical Hacker All-in-One Exam Guide (1st. ed.). McGraw-Hill Osborne Media.
- [MIC19]** Melanie Maynes, One simple action can take to prevent 99.9 percent of attacks on your accounts, <https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>
- [NIST21]** NIST, NIST Risk Management Framework RMF SP 800-53, <https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1>
- [OWA21]** OWASP, OWASP Top 10 Security Risks & Vulnerabilities, https://owasp.org/Top10/A00_2021_Introduction/
- [PRF21]** Proofpoint, State of the Phish 2021 report, <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
- [RAP21]** Rapid7, Common Types of Cybersecurity Attacks, <https://www.rapid7.com/fundamentals/types-of-attacks/>
- [SAN21]** SANS, Top new attacks and threats report, <https://www.sans.org/blog/sans-2021-threat-report/>
- [SSC21]** Security Score Card, Common cyber-attack vectors in 2021, <https://securityscorecard.com/blog/common-cyber-attack-vectors>
- [SHO09]** Shon Harris. 2009. CISA Certified Information Systems Auditor All-in-One Exam Guide (1st. ed.). McGraw-Hill, Inc., USA.
- [TOG18]** The Open Group (2018) TOGAF® Standard, Version 9.2, <https://pubs.opengroup.org/architecture/togaf9-doc/arch/>
- [VER21]** Verizon, Data Breach Investigations Report 2021, <https://www.verizon.com/business/resources/reports/dbir/>
- [UPG21]** Upguard, What is an Attack Vector? 16 Common Attack Vectors in 2021, <https://www.upguard.com/blog/attack-vector>