ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

D8.3 INTER-SECTOR PROTOTYPES DEMONSTRATION SURVEY

Lead author: Marco Pappalardo, CIRM

Submission date: 31 August 2021

PUBLIC

The work described in this document has been conducted within the ECHO project. This project has received funding by the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 830943

Title	European network of Cybersecurity centres and competence Hub for innovation and Operations
Acronym	ECHO
Number	830943
Type of instrument	Research and Innovation Action
Topic	SU-ICT-03-2018
Starting date	01/02/2019
Duration	48
Website	www.echonetwork.eu

D8.3 INTER-SECTOR PROTOTYPES DEMONSTRATION SURVEY

Work package	WP8
Lead author	Marco Pappalardo (CIRM)
Contributors	Gabriella Trombino (CIRM), Ewa Konieczna (VST), Michael Cooke (NUIM), Antonis Voulgaridis (CERTH), Marco Pappalardo (CIRM), Mike Anastasiadis (CERTH), Boris Marinov (TBS), Gregory Depaix (NG), Cyril Ceresola (NG), Marcin Niemiec (AGH), Rafal Kosciej (AGH), Bartlomiej Gdowski (AGH), Anagnostis Mengidis (CERTH), Pavel Varbanov (ESI CEE), Cagatay Yucel (BU), Cammisa Marco (EXP), Todor Tagarev (IICT), Petya Ivanova (IICT), Fabrizio De Vecchis (RHEA), Oleg Illiashenko (KAI)
Peer reviewers	Pavel Varbanov (ESI CEE), Matteo Merialdo (RHEA), Tiia Somer (TUT)
Version	V0.13
Due date	31/07/2021
Submission date	31/08/2021

Dissemination level:

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

Version history

Revision	Date	Editor	Comments
0.1	18/06/2021	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM)	Initial version of Deliverable and Table of Content
0.2	02/07/2021	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM)	Guidelines for writing all sections, initial content for Section 2.
0.3	12/07/2021	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM), Ewa Konieczna (VisionSpace)	Updated ToC. Removed section 4 which collapsed into section 3.
0.4	13/07/2021	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM), Ewa Konieczna (VisionSpace)	Updated ToC. Finetuned assignments, partially rearranged Section 3.
0.5	13/07/2021	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM), Ewa Konieczna (VisionSpace)	Finalized ToC. Rearranged Sections 3 and 4.
0.6	23/07/2021	Ewa Konieczna (VisionSpace)	Section 2
0.7	27/07/2021	Gabriella Trombino (CIRM)	Integratied contributions by tool owners in section 3.
0.8	11/08/2021	Marco Pappalardo (CIRM)	Integrated contributions by tool owners in section 3 and updates in other sections wrt D8.2.
0.9	19/08/2021	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM)	Integrated missing contributions in Section 3, finalized Sections 1 & 2. Review of Section 3.
0.10	20/08/2021	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM)	Review of Section 3.
0.11	24/08/2021	Ewa Konieczna (VisionSpace), Marco Pappalardo (CIRM), Gabriella Trombino (CIRM)	Reshuffled section 2, Improved Methodology and selection of survey tool.
0.12	28/08/2021	Michael Cooke (NUIM)	Improved Executive Summary. Revision of Section 1 and 2.
0.13	31/08/2021	Marco Pappalardo (CIRM)	Whole document review, managed peer reviewers comments.
1.0	31/08/2021	Matteo Merialdo (RHEA)	Document Closed

List of contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
All	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM)

Section	Author(s)
All	Michael Cooke (NUIM)
1	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM)
1.3	Antonis Voulgaridis (CERTH), Marco Pappalardo (CIRM), Michael Cooke (NUIM)
Section 2	Ewa Konieczna (VST)
3.1.1	Mike Anastasiadis, Antonis Voulgaridis (CERTH)
3.1.2	Ewa Konieczna (VST)
3.1.3	Boris Marinov (TBS)
3.1.4	Gregory Depaix (NG), Cyril Ceresola (NG)
3.1.5	Marcin Niemiec (AGH), Rafal Kosciej (AGH), Bartlomiej Gdowski (AGH)
3.1.6	Anagnostis Mengidis (CERTH)
3.1.7	Pavel Varbanov (ESICEE)
3.1.8	Cagatay Yucel (BU)
3.1.9	Cammisa Marco (EXP)
3.1.10	Todor Tagarev (IICT), Petya Ivanova (IICT)
3.1.11	Marco Pappalardo (CIRM)
3.1.12	Fabrizio De Vecchis (RHEA)
3.1.13	Oleg Illiashenko (KAI)
3.2	Antonis Voulgaridis (CERTH)
4	Marco Pappalardo (CIRM), Gabriella Trombino (CIRM), Ewa Konieczna (VST)

Keywords

INTER-SECTOR, PROTOTYPES, USABILITY, LIKEABILITY, INTEGRATION, USER SATISFACTION, SURVEY, TOOL.

Disclaimer

This document contains information which is proprietary to the ECHO consortium. Neither this document nor the information contained herein shall be used, duplicated, or communicated by any means to any third party, in whole or parts, except with the prior written consent of the ECHO consortium.

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Personal Data collected, used, and stored to produce the content of the deliverable were processed in compliance to requirements from the GDPR, according to ECHO Data Management Plan and ECHO Ethics deliverables.

Executive summary

The ECHO project (European network of Cybersecurity centers and competence Hub for innovation and Operations) aims to deliver an organized and coordinated approach to strengthen the proactive cyber defense of the EU having as key elements an effective and efficient multi-sector collaboration. In the aim of the project, a bunch of thirteen inter-sector prototypes have been defined with the goal to improve cybersecurity capabilities in the several domains. Each of these prototype, whose design and implementation is part of WP4 activities, address or simply face some of the Inter-sector Technical Cybersecurity Challenges identified in ECHO [D2.4][D4.2].

ECHO Consortium will also organise demonstration events available to the range of European organisations, industries and the public to gather feedback from participants of the execution of the ECHO demonstration cases, or joining the demonstration workshops and presentations, partners leading WP8 developed surveys examining users' satisfaction with the ECHO products. The aforementioned event will enable the chance to investigate and test the inter-sector tools by involving a wide and heterogeneous group of users.

In particular this deliverable deals with the survey used at gathering participant's expectations as well as feedback at first sight from participants of the inter-sector prototypes demonstration events allowing evaluation of prototypes effectiveness and applicability to the overall challenge of improving cybersecurity across the identified sectors.

The survey is demanded to enable the evaluation process of prototypes effectiveness and applicability to the challenge of improving cybersecurity across the identified sectors. With a higher detail, the survey should support ECHO project to:

- evaluate the effectiveness of the inter-sector prototypes;
- cross-check if the prototypes they meet the requirements of the European stakeholders as well as, in the case they do, identify modalities and corresponding level of match;
- estimate the degree of maturity and applicability of ECHO products and assets as well as demonstrated in relation to inter-sector prototypes and eventually support the identification of fixes for the gaps, towards the end of the ECHO project;
- investigate what challenges, included in the ones presented by WP4, the inter-sector prototypes face or address and how.

Surveys will be available to anyone interested in the project:

- members of the ECHO consortium and other cybersecurity projects
- ECHO Participants and collaborators who joined ECHO during the course of the project/ potential participants or collaborators who consider joining the project
- external specialists, advisors or stakeholders interested in the outcomes of the project
- potential end-users looking for adequate solutions to address their cybersecurity challenges

The initial feedback will be taken into consideration to improve tool's functionalities under task T7.3 'Early prototypes integration, installation and test' concluding the development of prototypes in July 2022.

All results will be summarized in *D8.5 Completed inter-sector demonstration surveys* in October 2022.

The survey has been implemented with Google Forms as a draft, an online survey included in Google G-Suite package.

At the time of writing this deliverable an additional implementation of the survey is under development on Qualtrics Core XM, which will be considered the main reference.

The building and rationale under the survey are depicted in Section 2. The survey will include a flexible number of questions, from nineteen to twenty-four for a single tool, depending on the tool which will be demonstrated. First eleven questions are to be considered common to all combination of tools. A tool-specific section, containing from eight to thirteen additional questions, will be activated once per selected tool. Descriptions per each tool and all related demonstrators will be included in Section 3 as well as specific questions to ask to survey respondents.

The survey begins with an introductory question asking the user to select the several inter-sector prototypes he is willing to test. In order to be flexible with the selection of prototypes, the number of question will be set dynamically during the respondent's activity. If the user selects just one prototype for testing, the questionnaire will be built by the initial eleven questions and the tool-specific questions (from eight to thirteen) for a maximum of twenty-four questions.

If the user chooses more prototypes to inspect or try, the initial eleven questions will be put at the beginning of the survey, followed by a number of tool-specific groups of questions, one group per tool selected. At the beginning of each group, the summary of the tool, the description of the demo and the link to watch/attend it will take place.

We expect users to complete the overall survey will take a maximum of 2.5 hours for any combination of three inter-sector prototypes, and max 1.5 hours in case of one prototype only (time depends on the selection made by the user). This time also includes the necessary reading of the tool summary and related demo description as well as the time needed to watch (video) or attend (real-time) the online demo.

The survey is available at the following link:

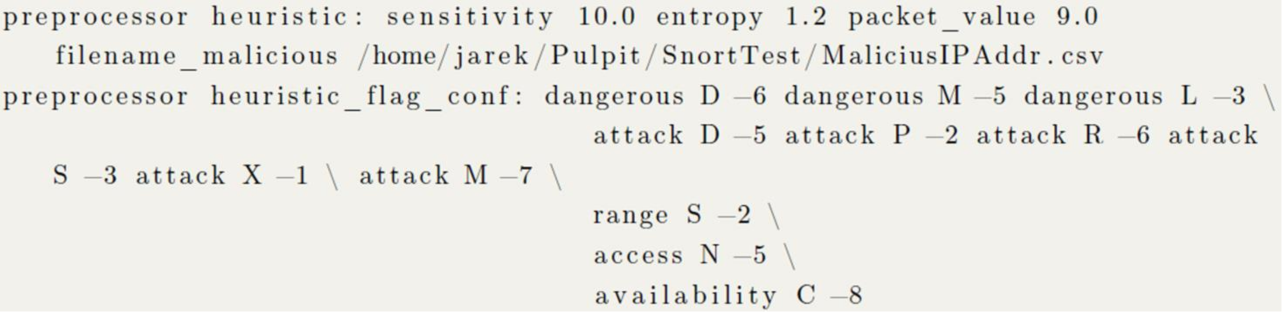
https://maynoothpsychology.qualtrics.com/jfe/form/SV_0NA8YpTGSYk86B8

Also the Google Forms version of the survey (working copy) is available here:

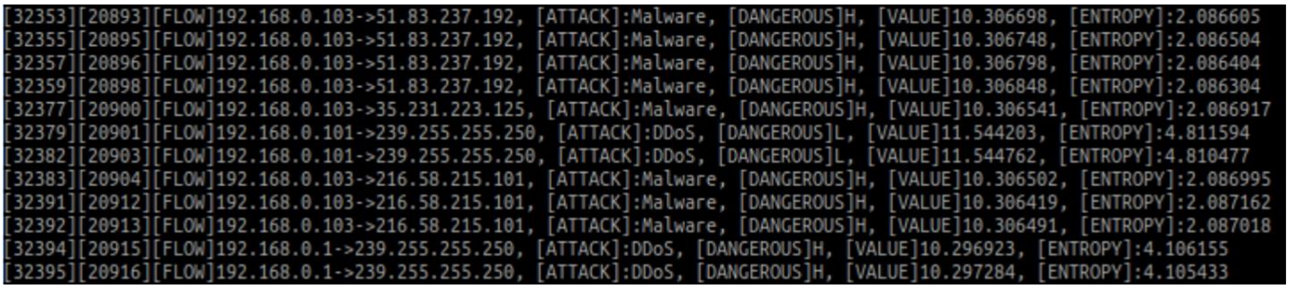
https://docs.google.com/forms/d/e/1FAIpQLSdM8fdKb41OMu-qZzIky_e-1AAeoh1ACY13q8U19XTy6_URhA/viewform

Table of contents

List of figures



```
preprocessor heuristic: sensitivity 10.0 entropy 1.2 packet_value 9.0
  filename_malicious /home/jarek/Pulpit/SnortTest/MaliciusIPAddr.csv
preprocessor heuristic_flag_conf: dangerous D -6 dangerous M -5 dangerous L -3 \
                              attack D -5 attack P -2 attack R -6 attack
  S -3 attack X -1 \ attack M -7 \
                              range S -2 \
                              access N -5 \
                              availability C -8
```



```
[32353][20893][FLOW]192.168.0.103->51.83.237.192, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306698, [ENTROPY]:2.086605
[32355][20895][FLOW]192.168.0.103->51.83.237.192, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306748, [ENTROPY]:2.086504
[32357][20896][FLOW]192.168.0.103->51.83.237.192, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306798, [ENTROPY]:2.086404
[32359][20898][FLOW]192.168.0.103->51.83.237.192, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306848, [ENTROPY]:2.086304
[32377][20900][FLOW]192.168.0.103->35.231.223.125, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306541, [ENTROPY]:2.086917
[32379][20901][FLOW]192.168.0.101->239.255.255.250, [ATTACK]:DDoS, [DANGEROUS]L, [VALUE]11.544203, [ENTROPY]:4.811594
[32382][20903][FLOW]192.168.0.101->239.255.255.250, [ATTACK]:DDoS, [DANGEROUS]L, [VALUE]11.544762, [ENTROPY]:4.810477
[32383][20904][FLOW]192.168.0.103->216.58.215.101, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306502, [ENTROPY]:2.086995
[32391][20912][FLOW]192.168.0.103->216.58.215.101, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306419, [ENTROPY]:2.087162
[32392][20913][FLOW]192.168.0.103->216.58.215.101, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306491, [ENTROPY]:2.087018
[32394][20915][FLOW]192.168.0.1->239.255.255.250, [ATTACK]:DDoS, [DANGEROUS]H, [VALUE]10.296923, [ENTROPY]:4.106155
[32395][20916][FLOW]192.168.0.1->239.255.255.250, [ATTACK]:DDoS, [DANGEROUS]H, [VALUE]10.297284, [ENTROPY]:4.105433
```

List of tables

1. Introduction

1.1 Purpose and scope of the document

As one of the four Pilot projects launched by the European Commission to establish and operate a European-level Cybersecurity Competence Network, the ECHO project (European network of Cybersecurity centres and competence Hub for innovation and Operations) aims to deliver an organized and coordinated approach to strengthen the proactive cyber defence of the EU. A key element of this is effective and efficient multi-sector collaboration. This makes Work Package 8 "Demonstration Cases" (WP8), which is required to prepare activities necessary for readiness to conduct open demonstrations of the identified technology roadmaps (E-EWS, E-FCR and inter-sector prototypes), extremely important. Within WP8, instantiation of systems and software in support of the demonstration and conducting a 'dry-run' of associated demonstrations take place. The results of the demonstration preparations, including traceability from demonstration plans to outcomes is captured in the Demonstrations Readiness Report.

This task includes preparation of surveys to be delivered during a series of demonstration workshops for both the core ECHO assets (the E-FCR and the E-EWS) and the inter-sector prototypes. Specifically, this deliverable deals with the survey(s) used to gather feedback from participants of the inter-sector prototypes demonstration events allowing evaluation of prototypes effectiveness and applicability to the challenge of improving cybersecurity across the identified sectors. The survey instrument for gathering data related to the ECHO core assets is contained in D8.2.

The objective of the survey in D8.3 is to collect the feedback from the participants of the inter-sector prototypes demonstration events allowing evaluation of prototypes' effectiveness and applicability to the challenge of improving cybersecurity across identified sectors. The feedback will be used to assess further improvements needed and steer the future development of those prototypes. So, this document collects a feedback from participants of the demonstration cases with the purpose of:

- Evaluating the effectiveness of the inter-sector prototypes and understanding if and how they meet the needs of European organisations and the market.

- Enabling the analysis of the degree of maturity and applicability of other ECHO assets demonstrated in relation to inter-sector prototypes and fix any gaps by the end of the ECHO project.

- Investigating what challenges, included in the ones presented by WP4, the inter-sector prototypes face or address and how.

This document also describes (Section 2) the methodology adopted for the implementation of the questions and the specific objectives of each of them, the target groups, as well as the procedure of applying the survey.

1.2 Structure of the document

This deliverable is structured as follows:

- Section 1provides a general introduction to the whole document. While highlighting the relations with other project deliverables and products, it describes the deliverable as part of the project high-level design and objectives.
- Section 2 details the methodology used to identify the questions to ask and the rationale underlying each of them. In addition to this, this section explains what are the target groups, the context and procedure for applying the survey. This section clarifies that the survey as a general part and a tool-specific part, dynamically adjusting with respect to any specific tool.
- Section 3 provides the deployment of the tool-specific part of the survey. Per each tool, it reads a description of the tool and of the specific demo as well as the list of the tool-related questions to be inserted in the survey with the respective rationale.
- Section 4 contains the conclusions and is finally devoted to summarize outcomes and elicit closing remarks.

1.3 Relation to other work in the project

The activities of WP8 in general, and the demonstration of the prototypes in T8.3 specifically, have a mutual dependency on other work packages within the project and therefore have a bearing on both how we devise and the survey and analyze and interpret the results.

All surveys produced under T8.3 and reported in the current document will be used to collect feedback on inter-sector prototypes (in this document also referred to as ‘tools’) developed within the WP4 ‘Inter-sector Technology Roadmaps’ and specifically task T4.3 ‘Early prototypes selection, research and development’.

From WP2, the demonstration cases that feature three of the prototypes – MonSys, SISP, and CyMs in demo cases 4 and 5 will rely on the scenarios and use-cases developed in T2.1 and the demonstration cases elaborated in T2.5. Task T2.3 also relies on the outcome of the demonstrations, including the relevant inter-sector prototypes, for the definition of the ECHO concept of operations for the assets which will make reference to the use of such prototypes and especially the data gathered from these surveys. Along with this the certification scheme and security targets will be a key input from T2.7.

Outcomes of the demonstrations, including the public response to the prototypes as represented in the data gathered through these surveys, will be of interest to WP3 in terms of the governance model.

The selection of prototypes followed a complicated selection methodology, reported in D4.4 ‘Inter-sector prototypes high-level design’, and was based on the objective of addressing inter-sector cybersecurity challenges identified during the research performed under WP2 ‘Multi-sector needs analysis’ and specifically T2.4 ‘Inter-sector technology challenges and opportunities’, and also T4.1 ‘Detailed analysis of transversal technical cybersecurity challenges’ with special focus on D4.1 ‘Transversal technical cybersecurity challenges report’ and D4.2 ‘Inter-sector technical cybersecurity challenges report’. A more detailed analysis on the connection between the inter-sector cybersecurity challenges and the selected prototype tools can be found in section 3.2.

Software development conducted within task T4.3, will take place until January 2022, upon completion of which the tools should be ready for demonstration to the public. The initial feedback collected will be taken into consideration to improve the tools' functionalities under task T7.3, 'Early prototypes integration, installation and test', concluding the development of prototypes in July 2022.

Roughly in parallel with the demonstration of other assets developed in the ECHO project, in T8.2, demonstration activities will be organized and conducted under the umbrella of WP8 'Demonstration Cases'. The Consortium has devoted task T8.3 'Early prototypes demonstration workshops' to focus on the demonstration of inter-sector prototypes specifically.

All results regarding the surveys will be summarized in *D8.5 Completed inter-sector demonstration surveys* in October 2022, while the overall results from the demonstrations will be summarized and reported *in D8.6 ECHO demonstration report* in January 2023.

1.4 Applicable and reference documents

The following documents contain requirements applicable to the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[GA]	Grant Agreement 830943 – ECHO	-	1.0	02/04/2019
[PH]	D1.1 Project Handbook	ECHO_D1.1_v1.42	1.42	20/10/2019
[PQP]	D1.3 Project Quality Plan	ECHO_D1.3_v1.4	1.4	23/04/2021

Table 1: Applicable documents

The following documents have been consulted for the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[D2.1]	D2.1 Sector Scenarios and Use Case Analysis	ECHO_D2.1_V1.0	1.0	1/11/2019 and 15/03/2020
[D2.2]	D2.2 ECHO Multi-sector Assessment Framework v.1.0.5 and v.2.4	ECHO_D2.2_v1.0.5 and ECHO_D2.2_v2.4	1.0.5 and 2.4	14/11/2019 and 18/06/2020
[D2.4]	D2.4 Inter-sector Technology Challenges and Opportunities	ECHO_D2.4_v1.0	1.0	31/01/2020
[D4.1]	D4.1 Transversal technical cybersecurity challenges report	ECHO_D4.1_v1.0	1.0	19/06/2020

Reference	Document Title	Document Reference	Version	Date
[D4.2]	D4.2 Inter-sector Technical Cybersecurity Challenges Report	ECHO_D4.2_v1.0	1.0	19/06/2020
[D4.5]	D4.5 Inter-sector prototypes v.2.1	ECHO_D4.5_v2.1	2.1	01/05/2021

Table 2: Reference documents

1.5 Intellectual Property Rights

Based on the legal framework provided in the ECHO Grant Agreement and the Consortium Agreement, ECHO specific IPR procedures have been established to protect the innovations and knowledge developed within this deliverable.

1.6 Glossary of acronyms

Acronym	Description
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
GA	Grant Agreement
IPR	Intellectual Property Rights
WP	Work Package
E-MAF	ECHO Multi-sector Assessment Framework
E-MAT	ECHO Multi-sector Assessment Tool

Table 3: Glossary of acronyms, initialisms, and abbreviations

2. Design of the Survey

This section introduces the methodology adopted for the implementation of the questionnaire(s). It also describes the several questions introduced by analysing respective objectives, introduces the rationale underlying any of these questions, discusses about the target groups, as well as the procedure of applying the survey. Clearly, the high-level goal of D8.3 is to develop an effective process for collecting feedback on inter-sector prototypes from target users so that information provided be available and useful to tools owner, decision makers, as well as helpful to tool owners in software optimization/improvement phase. The preferred format chosen is that one of an online survey to be published in the form of a questionnaire with both open and closed questions.

2.1 Objective of the survey

The design of the survey(s) to be delivered during demonstration workshops is built on top of a methodological approach which will be described in following pages. In particular, the surveys this deliverable deals with are to be used to gather feedback from participants of the inter-sector prototypes demonstration events. The survey(s) are demanded to enable the evaluation process of prototypes effectiveness and applicability to the challenge of improving cybersecurity across the identified sectors. With a higher detail, the survey(s) should support ECHO project to:

- to make user understand the objective of any specific tool, how it works, how the demo operates and what are its goals;
- evaluate the effectiveness and usability of the inter-sector prototypes;
- cross-check if the prototypes they meet the requirements of the European stakeholders as well as, in the case they do, identify modalities and corresponding level of match;
- estimate the degree of maturity and applicability of other ECHO assets demonstrated in relation to inter-sector prototypes and eventually support the identification of fixes for the gaps, towards the end of the ECHO project;
- investigate what challenges, included in the ones presented by WP4, the inter-sector prototypes face or address and how.

2.2 Methodology

At the time of the creation of this deliverable, software development of inter-sector prototypes is still ongoing. Since the survey foresees media incorporation to demonstrate selected prototypes, it will be fully completed once the demonstrated media is incorporated. A set of assumptions was made for the survey's development, considering the project's objectives and the development roadmaps of the inter-sector prototypes. In order to minimize effort spent in implementation/deployment of the survey(s) and make the target user provide comparable information even when using different tools, it has been decided to structure the questionnaire into two sections.

The first section, named *General purpose (questions) Section* (see Section 2.3.1), will be devoted to ask a set of eleven questions which will remain unchanged for all the inter-sector prototypes and demonstrations run by the user. This could allow the questionnaire to mainly be:

- agnostic, since they cannot depend on neither any specific tool/technology nor any specific technological challenge or opportunity;
- as general and generic as possible, allowing to evaluate aspects related to shared interests among all tool owners in order to enable comparison, grouping, etc. of information for deeper analysis; for this reason data collected should be as high-level/abstract and related to generic/common aspect as possible, in order to be collected for all tools easily;
- related to challenges depicted in [D4.1] and [D4.2] so to be tightly bound to analysis performed in WP4;
- referring to inter-sector tools enlisted in [D4.5] which are the ones the ECHO Project is interested to acquire feedback on and to evaluate effectiveness and efficacy;

Since the several tools are devoted to different goals, require proper input and provide a their specific output, it is quite obvious that there also is a set of non-shared questions which is necessary to the tool owner to evaluate features of the specific tool like completeness, effectiveness, integrability in existing systems, usability, likeability, etc. In particular, these are quality metrics which cannot be evaluated in a homogeneous manner among all the ECHO inter-sector tools. This additional set of questions will build the *Tool-specific (questions) section* of the survey (see Section 2.3.2). There a restricted set of eight to thirteen questions will be presented per each tool so that they can be dynamically loaded into the questionnaire with respect to any specific tool included in the given demonstration session/event. The number of questions depends on the specific requirements of each tool. The survey stipulates seven default questions and additional one to six questions depending on the tool. Some question will directly measure features like usability and completeness, others will enable the chance for an ex-post evaluation of the values obtained driving towards the estimation of the remaining features. The designed architecture for the survey will allow the ECHO Project team to minimize effort by building a single unified survey which partially and dynamically adapts to specific demonstrations and needs, ensuring anyhow the collection of both general/common interest data and tool-specific information. Due to this, this document will read “survey” when referring to the unified questionnaire from now on, despite “surveys” or “survey(s)” since it is clear the intention to build a unique source of information for the whole set of inter-sector prototypes.

We expect the participants can reach the questionnaire through a twofold path:

- either by visiting the ECHO web site and consider the information about the prototypes inside,
- or by participating in a workshop and thus receiving a deeper understanding about the prototypes and tools.

The added value in this design for the survey also lays in that fact that every deployment of the survey itself will contain the demo/event whom the survey relates to. In fact, it is foreseen that the demo of the selected inter-sector prototypes be run within the survey. For this reason, it is important that the Tool-specific section of the questionnaire be capable to provide enough information to user in order to make him/her understand the objective of the specific tool, how it works (at least from an external point of view), how the demo operates and what are its goals. So, in section 2.3.2, two subsections will be dedicated to describe any of the inter-sector prototypes and the related demonstrator, respectively. Tool descriptions are a summary of the more detailed contents which can be found in [D4.5] the more demanding reader should refer to.

2.3 Structure of the survey

The survey will be composed of the following parts:

1. General questions – questions to categorise the respondent and his/her general feedback towards the ECHO project and its outputs – listed in section 2.3.1 of this document

2. Tool-specific questions – questions to gather respondent's feedback towards the prototypes. Before answering this set of questions, the respondent will be given an opportunity to review the description of the tool and a presentation or recording of its demo once again.

   (a) Generic questions used to gather feedback for all prototypes – listed in section 2.3.2
   (b) Additional questions addressing the specific character of each prototype – further described in particular subsections of section 3.

General questions will help the team to analyse the results of the survey in a holistic manner.

Tool-specific questions will help the team evaluate the prototypes' effectiveness and applicability to address challenges identified in task T4.1 "Detailed analysis of common technical security challenges" which was considered when selecting prototypes for development. The matrix of challenges each prototype aims to address can be found in section 3.2 of this document.

In the next sections the entire list of questions will be presented, by separating them in the two groups relating to the two sections of the survey. Per each of them, the specific question will be discussed as well as the rationale leading to it. Similarly, the category of the expected reply will be described (textbox, choice, multiple choice, etc.) as well as the possible list of items for choices when a reply from an item list (choice or multiple choice) is expected.

In the next section the following typographical rules will be used:

- bold and italic for the question text (e.g. ***What is your position in your organisation?***)
- bold and square brackets for the expected category of answer (e.g. **[textbox]**)
- a value list of items separated by commas (,) enclosed in square brackets for the lists (e.g. "[Monday, Tuesday, Wednesday]").

2.3.1 General purpose Section

The first part of the questionnaire consists of general questions to categorise the respondent and his/her general feedback towards the ECHO project and its outputs. Specifically, these questions should be:

- devoted to identify the demo user who is filling the questionnaire: the target group provides a quite large set of items so it is important to identify and assign the proper group for the specific user;
- providing information on the organisation and county the user belongs to or live in;
- related to the experience the user lived when running the demo;
- providing information on visibility of ECHO outcomes;

- evaluating the capability of the demo to fulfil the needs of user's organisation and whether it could lead to an easy integration design activity with existing tools in original organisation.

General questions

The first five questions will help us to analyse the feedback with regards to the category of the respondent. The analysis will be used as input for the dissemination and exploitation strategy.

Question #1 – Job title

What is your position in your organisation?

Expected category of answer: **[textbox]**

Even the survey will be anonymous, it is important to collect information on the role and responsibilities belonging to the respondent (see Question #4).

Question #2 – Industry type

In what sector does your organisation operate?

Expected category of answer: **[choice]**

Option list for answer: [Finance,
Healthcare,
Manufacturing,
Transportation,
R&D,
ICT,
Space,
Defence,
Public administration/sector,
Energy,
Water,
Food,
Chemical and Nuclear Industry,
Other]

If the user selects "Other", a textbox appears asking for a deeper explanation.

This question is fundamental to grab information on the domain of operation of the responding organisation.

Question #3 – Work country

Which country do you work in?

Expected category of answer: **[textbox]**

Option list for answer: [a list of all countries in the world]

This question allows to get information on the country the respondent is located. This will enable the tuning of the follow-up analysis on proper national or international regulation.

Question #3.b – Company headquarters country

Which country is your company headquarters located in?

Expected category of answer: **[choice]**

Option list for answer: [a list of all countries in the world]

The previous question is not enough to depict the regulatory landscape the user is subjected to since, e.g. in the case of multinational organisation, information on headquarter location is needed. This is why a further question is asked on company headquarters. There are several implicit reasons by which it is important to understand the difference between the person working place of the headquarter of the company.

Question #4 – Work department

Which department do you work in?

Expected category of answer: **[textbox]**

Even the survey will be anonymous, it is important to collect information on the role and responsibilities belonging to the respondent (see Question #1).

Question #5 – Company size

How many employees does your company have?

Expected category of answer: **[choice]**

Option list for answer: [1-9, 10-49, 50-249, 250-499, 500 or more]

Question #6 – The visibility of ECHO

How did you find the ECHO network website?

Expected category of answer: **[choice]**

Option list for answer: [I am a member of the ECHO consortium,
Through another H2020 project,
Through common business partner/stakeholder,
Through LinkedIn/social media,
Search engine,

Other]

In fact, if the user selects “Search engine”, a follow up question appears asking what the search phrase was. The user should reply through a textbox. If “Other” is chosen, the textbox should require further clarification.

Question gathers feedback regarding the effectiveness of our dissemination efforts with regards to the respondent (category of respondent mapped in Q1-5, and respondent’s interests mapped in the rest of the questionnaire).

Question #7 – Workshop quality set

How do you rate the quality of the workshop/event according to the following aspects? If you did not attend any please set the Grade of Participation to “1 - Not attended”.

Expected category of answer: **[set of choice 1-to-5] or [set of 1-to-5 sliders]**

The survey is usually administered following an ECHO workshop or an event the Project is organizes or is invited to. The quality of the workshop will be evaluated through the six following elements, which will be estimated as described in the following:

- Grade of Participation [1 means “Not attended”; 2 means “low”; “5 means “high”]
- Quality of the workshop structure [1 means “not at all”; 5 means “very good”]
- Quality of the speaker [1 means “boring”; 5 means “very good”]
- Quantity of information [1 means “no clear at all”; 5 means “very clear”]
- Level of interaction [1 means “not enough”; 5 means “too much”; 3 means “perfect”]
- Length of the workshop [1 means “not short”; 5 means “too long”; 3 means “perfect”]
- The overall workshop [1 means “not good”; 5 means “very good”]

In the case the user fills the survey autonomously, he/she is requested to set the Grade of Participation to the workshop to “1”. All remaining replies will be ignored.

Question #8 – Added value of ECHO solutions

Would you say that ECHO solutions can bring an added value for your organisation?

Expected category of answer: **[choice]**

Option list for answer: [Yes, Partially, No]

ECHO solutions have been presented during the workshop so the user can state some initial evaluation of the chances to add value to organisation. The question was added to verify whether the respondent may benefit from the use of ECHO solutions. The analysis of results in conjunction with questions 1-5 will help us aim the exploitation strategy.

Question #8.b – Added value of ECHO solutions

Can you explain in few lines the reason of this answer?

Expected category of answer: **[textbox]**

This question underlines the need of having a deeper feedback to be exploited ex-post.

Question #9 – Coverage of inter-sector prototypes

Does the scope of demonstrated inter-sector prototypes meet your expectations? If no, please explain.

Expected category of answer: **[choice]**

Option list for answer: [Yes, Partially, No]

If the user selects “Partially” or “No”, a textbox appears asking for a deeper explanation.

The rationale for this question is to check whether the variety of inter-sector prototypes meets the expectations of potential users. It also verifies whether the way tools are presented is adequate.

Question #10 – General Usability of the Demo

Would you say that the website demonstrates the ECHO solutions in understandable and clear way? If it does not, what can be improved?

Expected category of answer: **[choice]**

Option list for answer: [Yes, Partially, No]

If the user selects “Partially” or “No”, a textbox appears.

The rationale for this question is to check whether the way tools are presented is adequate.

Question #11 – Future intention

Are you interested in collaboration with ECHO?

Expected category of answer: **[multiple choice]**

Option list for answer: [I would like to offer my expertise in cybersecurity to improve ECHO solutions,
I would like to offer my expertise in software development to improve ECHO solutions,
I would like to learn more about solutions to protect my organisation,
I would like to join the demonstration workshop,
No, thank you]

If the user selects one of "I would like to" options, a textbox appears, so that respondent can leave his/her contact information and state the area of interest (optional).

The question helps us evaluate the intentions of the respondent and whether demos attracted the attention of a potential partner, consumer or another stakeholder.

2.3.2 Tool-specific Section

As described when discussing the design of the survey, this section is expected to be tightly related to the inter-sector tools. As described in survey methodology (see Section 2.2), per each tool a short summary is provided as well as the description of the demonstration. In the following sub-sections, the several elements of the Tool-specific Section will be presented. Some of them will be defined in an abstract way. In fact, questions specific to each given prototype have been provided by tool owners and can be found in Section 3.1.

As the reader can see, the Tool-specific Section is composed by three elements:

- the description of the inter-sector tool,
- the description of the tool demonstrator,
- the set of tools-dedicated questions.

When deploying the survey, these elements will be dynamically allocated in the web survey to build the Tool-specific Section. So, Section 2.3.1 and Section 2.3.2 simply introduce the need to provide and take into consideration the descriptions of the tool and the demo. The tool-specific content to fill the two sections in the survey correspondingly will be found in Section 3.1, within the specific 3.1.x sub-section (one per inter-sector prototype). The same will happen for Questions #16 and #17 which will be presented as placeholders in this Section. They will be deployed within the corresponding Section 3.1.x in a tool-specific manner.

The choice to mix demonstrators and survey is the clear added value for D8.3 questionnaire. An online demonstrator provides the chance to try a software out in real-time and putting it directly within the online survey enables the collecting of immediate first-hand responses and feedback.

Description of the Tool

This subsection contains a summary of the tool, its design, operation, goals in an immediately comprehensible format to the user. The constraint is that the tool and any necessary information to try it out must be provided in 2 written pages and 2 figures max.

All the tool-specific descriptions are inserted in the 3.1.x subsection in the next chapter.

Description of the Tool Demo

A fully understandable and enough comprehensive demonstration of the tool will be provided. This description will be put as an introductory text to the demo in the online survey.

All the demo descriptions are inserted in the 3.1.x subsection in the next chapter.

Tools-related questions

The second part of the questionnaire consists of questions to gather respondent's feedback towards the prototypes. Before answering this set of questions, the respondent will be given an opportunity to once again review the description of the tool and a presentation or recording of its demo.

This section contains a set of tools-related questions. Some of them can be considered to be valid for all the tools (Questions #12, #13, #14, #15, #18 and #19). In addition to this, based on the nature of each prototype, two more questions (Questions #16 and #17) are more "focused" and offer the chance to collect dedicated feedback on uncommon or tool-specific capabilities.

- Question #16 inquires to verify how the added value of the tool as perceived by the respondent compares with the intended goal of the tool. The list of cybersecurity challenges tools aimed to address can be found in Section 3.2 of this document. The cybersecurity challenges listed in the Table 11 will serve as a basis for the reply options of Question #16.
- Question #17 and its possible extensions aim to address inquiries of tool owners specific to the prototype developed by them. As an example, from a malware analysis tool a user might expect some specific functions while for an intrusion detection system other features are more important.

These two questions offer the chance to ask dedicated questions and collect feedback through them. Although the "core" questionnaire still remains more general (questions to measure the usability, completeness, innovation, etc of the tool are still general), questions #16 and #17 may provide a chance for a more effective approach.

Question #12 – Usability of the tool

How do you rate the usability of the tool? *Note: for the assessment of usability, please consider: does the tool seem to be effective, efficient, easy and intuitive**.***

Expected category of answer: **[1-to-10 choice]**

Option list for answer: [slider from 1 to 10]

Inter-sector prototypes should simplify the daily tasks of cybersecurity analysts and other professionals. The demo should clearly explain how to use the tool. Gathered feedback will let us know whether respondent perceived its usability as high or low.

Question #13 – Usefulness of the tool

How do you rate the usefulness of the tool? *For the assessment of usefulness, please consider how, in your opinion, this tool is useful to tackle cyber security issues in nowadays market.*

Expected category of answer: **[1-to-10 choice]**

Option list for answer: [slider from 1 to 10]

Gathered feedback will let us know whether respondent perceived tool usefulness as high or low.

Question #14 – Completeness of the tool

How do you rate the completeness of the tool? *For the assessment of the completeness, please consider: does the tool seem to be ready to use, not lacking important functionalities for the application it is aimed for?*

Expected category of answer: **[1-to-10 choice]**

Option list for answer: [slider from 1 to 10]

Under the ECHO project we targeted at least two inter-sector prototypes to reach TRL6 technology demonstrated in relevant environment. The questions gathers feedback of perceived TRL of the prototype.

Question #15 – Innovation of the tool

Would you say that the tool is innovative? *For the assessment, please consider: are there many similar solutions on the market, does the tool address the newest emerging cybersecurity threats, does the tool address needs of organisations these days?*

Expected category of answer: **[1-to-10 choice]**

Option list for answer: [slider from 1 to 10]

The question aims to gather feedback about the potential for the future success of the tool. It will help us evaluate the potential of prototypes and navigate our allocation of future efforts.

Question #16 – Inter-sector Technological Challenges

Would you say that the tool successfully addresses following cybersecurity challenges? Select all that apply.

Expected category of answer: **[multiple choice]**

Option list for answer: [per each tool the list of transversal and inter-sector technological challenges in Table 11 should be shown]

Question aims to verify whether inter-sector prototypes selected for development address the cybersecurity challenges, according to their original intentions. Mapping of inter-sector prototypes and cybersecurity challenges can be found in section 3.2. Reply options will be dynamically adjusted based on the tool selected by the respondent.

Question #17 – Tool-specific Question #17.1 - #17.6 (optional)

This part of the questionnaire will be devoted to tool-specific questions aiming to assess the specific characteristics/features of a tool. It will be dynamically adjusted based on the tool selected by the respondent. The subset of questions categorized by the tool can be found within sub-section 3.1.x in the next chapter.

Question #18 – Chances or obstacles for Integration

Would you consider using this tool in your organisation?

Expected category of answer: **[1-to-10 choice]**

Option list for answer: [Yes, it seems to be useful for my organisation
No, it does not offer any value-added to my organisation
Other]

The question aims to gather feedback, from yet another perspective, on what is the potential of this inter-sector prototype.

If the user selects "Yes, […]" or "No, […]", a textbox appears with different requests to better clarify. When responding positively the user will be asked

If yes, can you tell how?

Expected category of answer: **[textbox]**

When responding negatively the user will be asked

If no, can you tell why?

Expected category of answer: **[textbox]**

When selecting "Other" the user will be asked to explain the choice with another textbox

Expected category of answer: **[textbox]**

Question #19 – Request for further contacts

Would you like to learn more about the prototype or take part in its future development? Leave us your contact information with a short description.

Expected category of answer: **[textbox]**

The question aims to liaise with potential future stakeholders.

2.4 Technology adopted and dissemination of the survey

The reason why a potential user will positively approach the ECHO demos and thereupon fill the survey is that the survey will be presented as part of the learning process. The selected technology and methodology will facilitate him/her not only to provide the necessary information to ECHO but will be seen as a perfect complement of the study and evaluation activity. The questions will open to further questions which will move towards the organisation the user belongs to. This a substantial and valuable outcome for the ECHO network.

As described in the Demonstrations readiness report [D8.1], the project stipulates five main ECHO demonstration cases:

- E-EWS use for reference library exchange
- E-EWS use for incident coordination response
- E-FCR use for cyber-skills education and training
- E-FCR use for cybersecurity certification of new technologies
- E-FCR use for R&D activities of the technology roadmap

As mentioned in [D8.2], surveys related to E-EWS and E-FCR will be provided to participants directly after the demonstration event. However, the main ECHO demonstration cases listed above focus mainly on the functionalities of E-EWS, E-FCR and other non-technical assets. They do not demonstrate the full scope of inter-sector prototypes. Even though certain prototypes can be demonstrated to some extend during main demonstration cases, the consortium has agreed to organise an additional event to demonstrate all prototypes developed during the project. Among considered options, the prevailing one was to devote the space for the presentation of inter-sector prototypes on the project website. Description of prototypes, presentation slide decks and videos will be deployed at https://echonetwork.eu/. The website will also include questionnaires related to given prototypes.

The questionnaire will also accompany additional events or workshops including demonstration of one or more inter-sector prototypes.

In contrast with E-EWS or E-FCR surveys described in [D8.2], the inter-sector demonstration survey aims to evaluate the effectiveness and applicability of a higher number of technical solutions developed within the ECHO project. Thereof, one agnostic questionnaire would not adequately encapsulate the feedback provided for each prototype. To avoid the creation of too many overlapping questionnaires, the consortium will prepare an extended questionnaire including the dynamically adjusted variation of questions specific to the selected prototype.

An interactive survey can be made available through several technologies. Among the ones already available on the market some were evaluated and, in case of positive evaluation, tested with a simplified version of the survey (only for Qualtrics Core XM and Google Forms). In order to determine whether a given tool was suitable for the objective to host our survey, we evaluated several features for free tools:

- limits in the maximum number of respondents;
- limits in the maximum number of questions;
- integrability with CRM or marketing suites;
- availability of Templates;
- capability to export data.

In addition to this, in order to host the survey, the software tool must provide the following functionalities:

- capability to show/alter questions depending on the response to a previous question;
- capability to show a question/sub-question structure, where sub-question depends on a condition involving response to the main question.
- capability to enable/disable groups of questions depending on the response to a previous question;
- capability to enable/disable groups of questions depending on the responses to a multi-choice question;
- capability to equivalently place groups including different number of questions depending on the response to a previous question.

As said, only Google Forms and Qualtrics Core XM demonstrated to have most of the features enlisted above. Even Qualtrics is a primary actor on the online survey landscape, unfortunately it has limited number of questions and respondents for the license free version. That led us to focus also on Google Forms which provides a very effective solution to manage tool-specific questions through the iterative loop construct enabling a group of questions depending on the response to a multi-choice preliminary question, while a business license for Qualtrics Core XM was made available for the official deployment of the survey.

The survey is available at the following URL (Qualtrics):

https://maynoothpsychology.qualtrics.com/jfe/form/SV_0NA8YpTGSYk86B8

Also the Google Forms version of the survey (working copy) is available here:

https://docs.google.com/forms/d/e/1FAIpQLSdM8fdKb41OMu-qZzIky_e-1AAeoh1ACY13q8U19XTy6_URhA/viewform

2.5 Target groups

Surveys will be available to anyone interested in the project.

- Members of the ECHO consortium and other cybersecurity projects
- ECHO Participants and collaborators who joined ECHO during the course of the project/ potential participants or collaborators who consider joining the project
- External specialists, advisors or stakeholders interested in the outcomes of the project
- Potential end-users looking for adequate solutions to address their cybersecurity challenges

All feedback enabling the accurate assessment of the efficiency and applicability of our solutions in relation to their purpose is welcome.

2.6 Ethics

Prior to the dissemination of the final surveys they will be submitted to the Maynooth University (NUIM) ethics committee for social scientific research for approval. The administration of the survey will be conducted in a manner consistent with the requirements of GDPR, as well as the code of conduct of the Psychological Society of Ireland (PSI) and the Maynooth University principles for ethical social-scientific research.

2.7 Evaluation of the results

As described in the previous section, surveys will be placed on the project website along materials demonstrating the usage of inter-sector prototypes. The section devoted to prototypes and related documentation will be published upon the finalization of task T4.3 'Early prototypes selection, research and development' in January 2022.

The initial feedback will be taken into consideration to improve tool's functionalities under task T7.3 'Early prototypes integration, installation and test' concluding the development of prototypes in July 2022.

All results will be summarized in *D8.5 Completed inter-sector demonstration surveys* in October 2022.

3. Inter-sector prototypes

The objective of the survey in D8.3, as described in Section 1.1, is to collect the feedback from the participants of the inter-sector prototypes in order to foster improvements and future development, from one side, and assess effectiveness and applicability to the challenge of improving cybersecurity across identified sectors, on the other. The feedback will allow to:

- evaluate effectiveness of inter-sector prototypes;
- support analysis on maturity and applicability of ECHO assets in relation to inter-sector prototypes;
- investigate the capabilities to face and address challenges.

Consequently, the aim of the deliverable is that to explore specific aspect of the Inter-sector Prototype identifying strengths and weaknesses of tools. So, it is necessary to introduce each tool in the survey, when the user selects it for the demo. Similarly, also a description of the demo which is going to take place must be preliminarily presented.

3.1 Description of Prototypes

3.1.1 Penetration Testing Tool

Description of the Tool

The main scope of the Penetration Testing tool is to provide a fully automated vulnerability scanner that detects and reports vulnerabilities including (web) application vulnerabilities, network protocol vulnerabilities, operating system vulnerabilities, misconfiguration vulnerabilities. This tool not only complements the role of a penetration tester but also automates tasks that can take hours to test manually, delivering results with the fewest possible false positives.

The Penetration Testing tool has four basic functionalities. In the first stage, the tool scans the network to identify open ports in the target by using *nmap scanner* or *massccan*. In the meantime, the *nmap-vulner* plugin identifies vulnerabilities on these open ports. By using the results of the first stage, the second stage further enumerates the services running on these open ports to identify possible security holes on the system. In the third stage, the tool based on the results from the scanning and enumeration stage will use the *metasploit framework*, *sqlmap*, and other custom-made tools and plugins, to perform automated attacks on the services. In the fourth and last stage, the tool presents the results to the user in a friendly Web Interface.

The penetration testing process can be broken down into four stages:

The first stage is the **Scan-Enumeration gathering**. At this stage, the tool will perform port scanning on the target under an agreement for privacy. Specifically, the PT (Penetration Testing) tool will collect details about the open ports, networks and services of the target. The tool performs three stages of scanning:

- *nmap scanner* for top 100 TCP/UDP ports;
- *nmap* or *masscan* in all 65536 ports of the system;

- scans for vulnerabilities on open ports by using *nmap-vulners*;
- Ncrack for network authentication cracking.

In the second stage, the tool will perform further enumeration on each of the results collected in the first stage. For example, if the target has HTTP/HTTPS services on 80/tcp & 443/tcp ports, the tool will attempt to find more directories, files and services by using:

- **gobuster** to brute force directories and files;
- **Nikto** for identifying common web app vulnerabilities;
- if the HTTP service is secure (HTTPS), the tool will also use *sslscan* to enumerate server key exchange groups, server signature algorithms, SSL/TLS protocol version, etc.

The third stage is **active vulnerability validation and exploitation**. At this stage, the tool based on the results from scanning and enumeration will use the *metasploit framework*, *sqlmap*, and other custom-made tools and plugins, to perform automated attacks on the services. For example, if we have found a potential vulnerability while scanning and there is an exploit on ExploitDB, *metasploit* will automatically attack the service by using the corresponding exploit. Lastly, *metasploit* will return the results according to the success or failure of the attack. The main purpose of the active vulnerability validation stage is to reduce the false positives.

In the final stage, the tool will present the results in a friendly user interface (UI). The UI will provide the user with an analytical report of the identified vulnerabilities, open ports and problems in their system.

Since privacy is a major subject in general and in the ECHO project in particular, the PT tool designed in such a way that will only provide access to the vulnerability scanning/exploitation results under a privacy agreement. The results of the four stages will be shared only between the tool and the company. These results will be stored encrypted in a database to minimize any concern of cyber security threats including data breaches.

Capabilities

A list of the basic tool's capabilities is shown in the following table.

Category	Functionality	Description	Note
Port Scanning	**The tool scans the target by using popular scanners like nmap to identify open ports and services.**	Identifies open ports and services available on the target.	To identify open ports the tool uses the *nmap scanner*.
Vulnerability Scanning	**The tool based on the port scanning results inspects for vulnerabilities on the open ports.**	Inspects potential points of exploitation to identify security holes.	Perform vulnerability scanning by using the ncrack, nmap-vulners plugin and nikto.
Information Gathering	**The tool gathers any kind of information to verify the identified vulnerabilities.**	Gathers a different kind of information against the targeted victim or system by using various	The tool enumerates all the services to gather information. Various tools will be used here, such as gobuster,

Category	Functionality	Description	Note
		open-source tools and techniques.	sslscan, enum4linux, dnsscan.
Vulnerability validation and exploitation	**The tool attempts to attack the target to reduce the chance of false positives.**	Verifies the existence of vulnerabilities by actually attacking the target.	It searches for possible exploits based on the vulnerabilities reported in the previous stages. It then uses these exploits to verify the existence of vulnerabilities.
Detection Report	**The tool presents all the above results in a friendly UI.**	In the final stage, the results from all the previous stages will be presented to the user in a friendly UI.	

Table 4: Capabilities of the Penetration Testing Tool

User interface/Mockups

In this section, the Penetration Testing Tool's user interface (UI) will be presented. The UI consists of 5 views, namely Net Discover, Scanning, Fingerprinters, Web Exploiters and Report.

Net Discover

Net Discover is the first and default view when the user starts Penetration Testing Tool. As depicted in Figure 1, Net Discover creates a topology of the local area network. By clicking the Local Network button, a topology of the user's network is created, with all the available devices in the local network. At the centre of the topology, the user's IP is depicted, while the connections are the available/visible devices. Each device is characterized by an IP address and a simple icon. Moreover, on the right side, a column appears with all the available information depicted as a list. Finally, a timestamp of the scan is shown on the upper right corner of the topology, helping the user refer to this scan at any time in future.

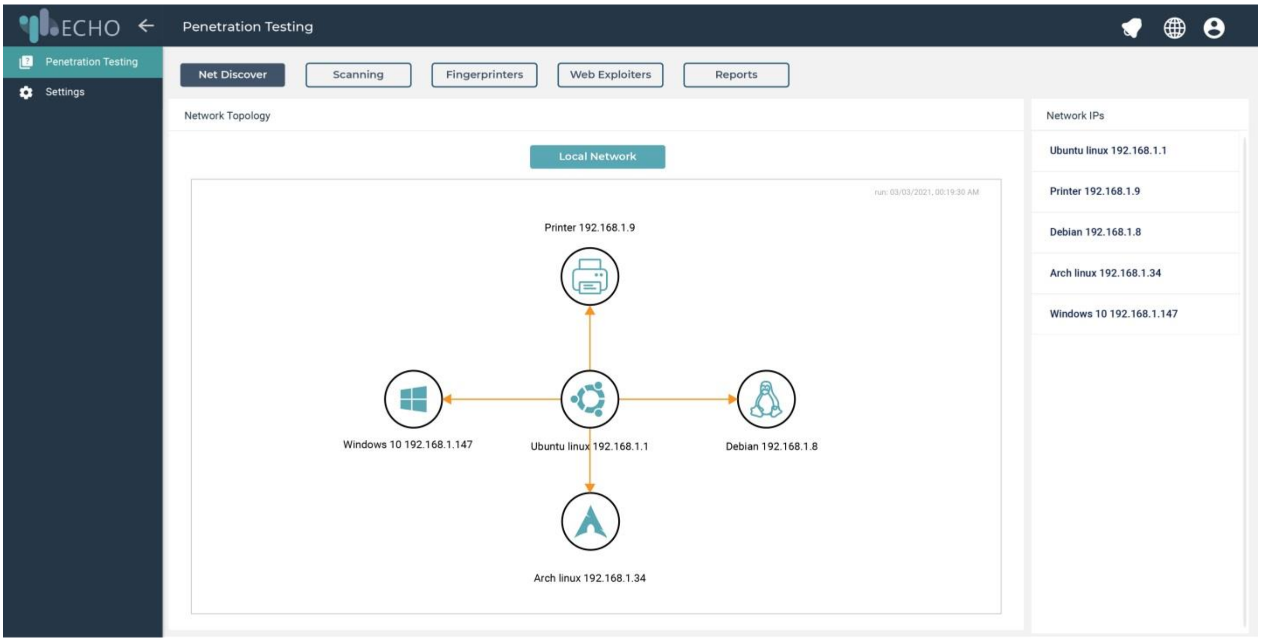
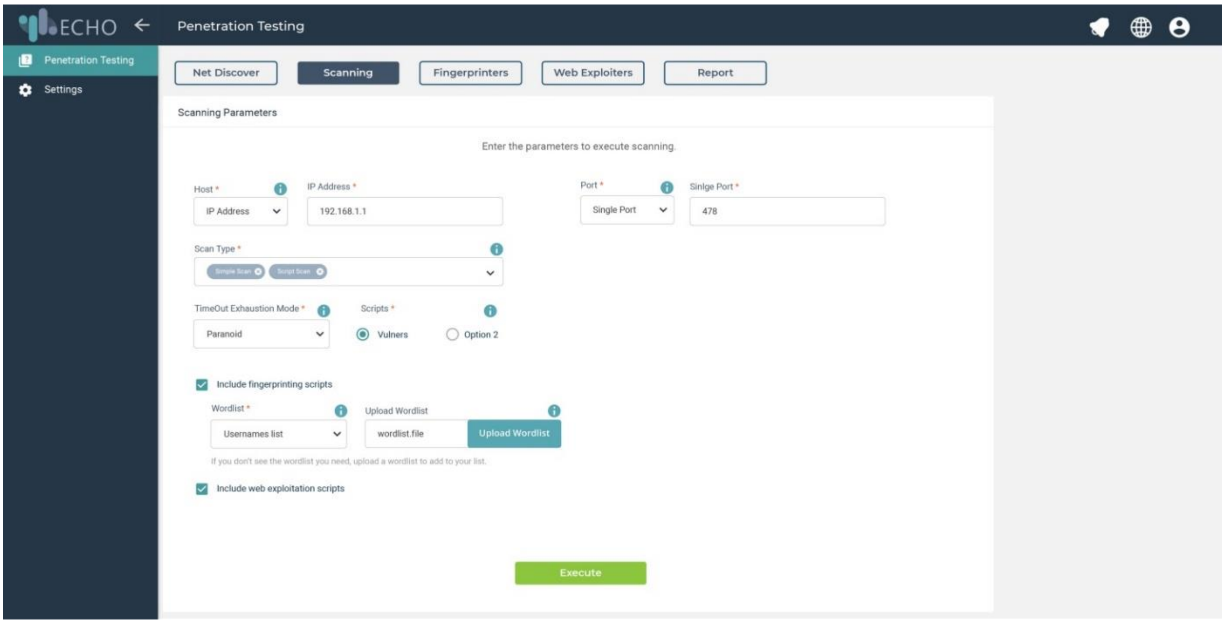


Figure 1: Net Discover.

Scanning

The second view is Scanning, where, as depicted in Figure 2, the user has to enter some parameters to start scanning the network. First of all, the user needs to select the Host from the dropdown menu. Then, depending on the choice, the user should input the specific parameters e.g IP address. Secondly, the Port type must be selected and defined in the corresponding cell. Finally, the Scan Type, the Time Out Exhaustion Mode and the Scripts parameters should be selected. Optionally, the user can include the fingerprinting phase or web exploitation phase in the scanning. If the fingerprinting phase is enabled then the user can select a wordlist either from the drop-down menu or upload a new wordlist according to their needs. The results of this tab will be shown on the Report tab.



Scanning Parameters

Enter the parameters to execute scanning.

Host *: IP Address

IP Address *: 192.168.1.1

Port *: Single Port

Sinlge Port *: 478

Scan Type *: Simple Scan, Script Scan

TimeOut Exhaustion Mode *: Paranoid

Scripts *: ● Vulners ○ Option 2

☑ Include fingerprinting scripts

Wordlist *: Usernames list

Upload Wordlist: wordlist.file

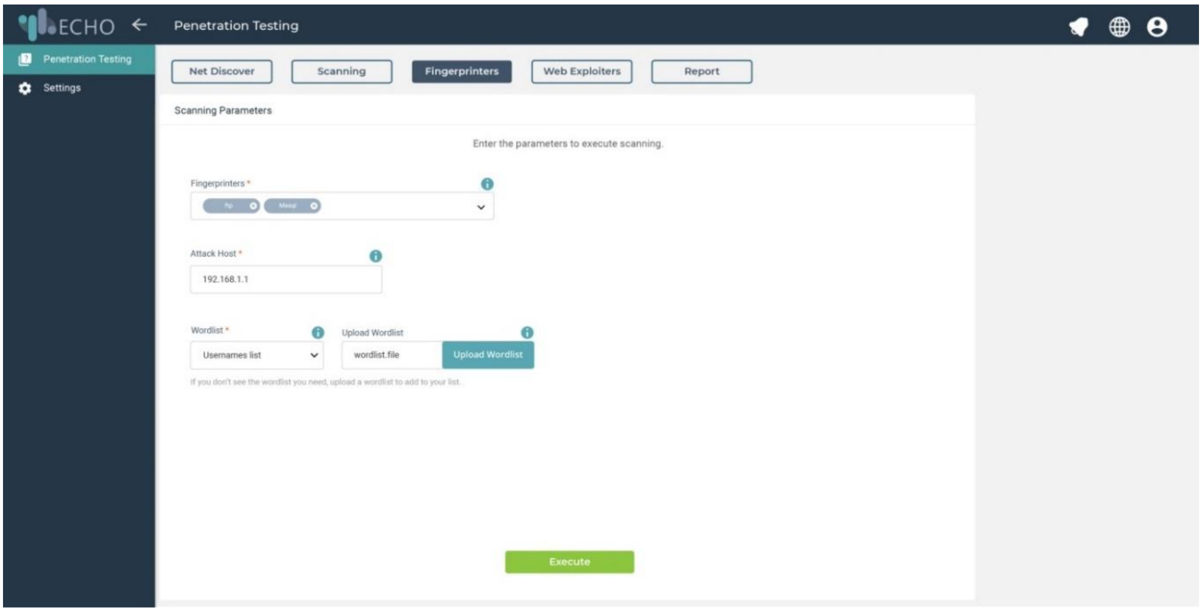
If you don't see the wordlist you need, upload a wordlist to add to your list.

☑ Include web exploitation scripts

Figure 2: Scanning.

Fingerprinters

The Fingerprinters view is depicted in Figure 3. The fingerprinters tab can be selected on the scan view, as described previously, or run independently from this view. Again, the user has to select a list of six fingerprinters to run from a drop-down menu, the host to attack, and a wordlist. Specifically, the user can brute force up to six services *ssh*, *mysql*, *ms-sql*, *postgresql*, *ftp* and *samba* to find common credentials. The results of this tab will also be shown on the Report tab.



Scanning Parameters

Enter the parameters to execute scanning.

Fingerprinters *: ftp, Mysql

Attack Host *: 192.168.1.1

Wordlist *: Usernames list

Upload Wordlist: wordlist.file

If you don't see the wordlist you need, upload a wordlist to add to your list.

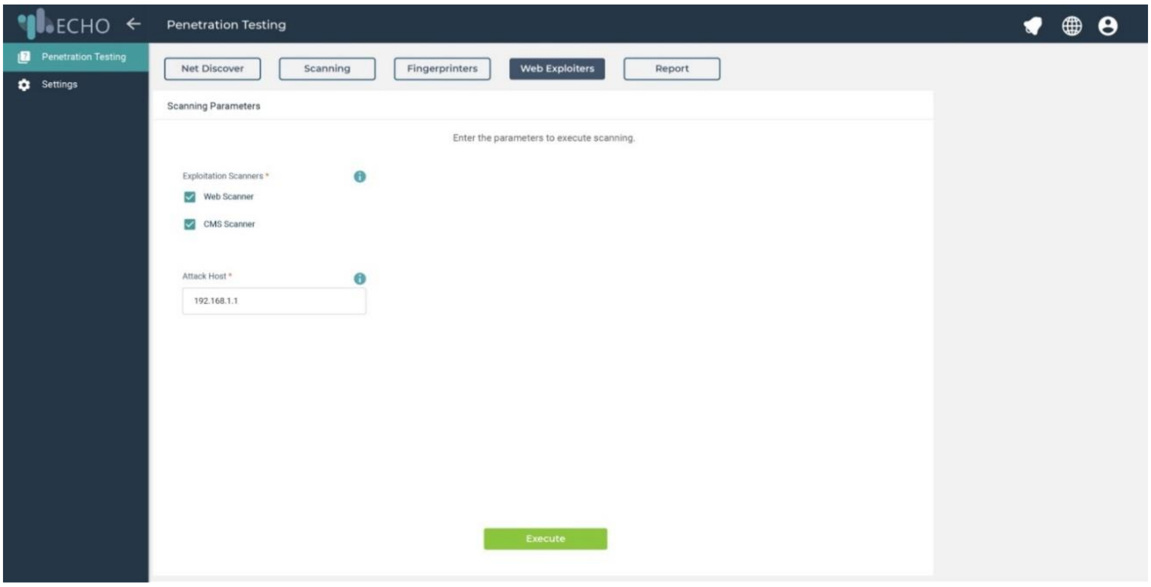
Figure 3: Fingerprinters.

Web Exploiters

The fourth view, depicted in Figure 4, is the Web Exploiters. Again, this tab can run alongside the scan tab, or independently from this view. The user needs to select an exploitation scanner and a host to attack. Two scanners are provided:

- the first one scans web applications to find common vulnerabilities, files and directories;
- the second one scans Content Management Systems to find identified common vulnerabilities.

The results of this tab will also be shown on the Report tab and consist of two HTML templates with the results of each one of the vulnerability scanners.



Scanning Parameters

Enter the parameters to execute scanning.

Exploitation Scanners *

☑ Web Scanner

☑ CMS Scanner

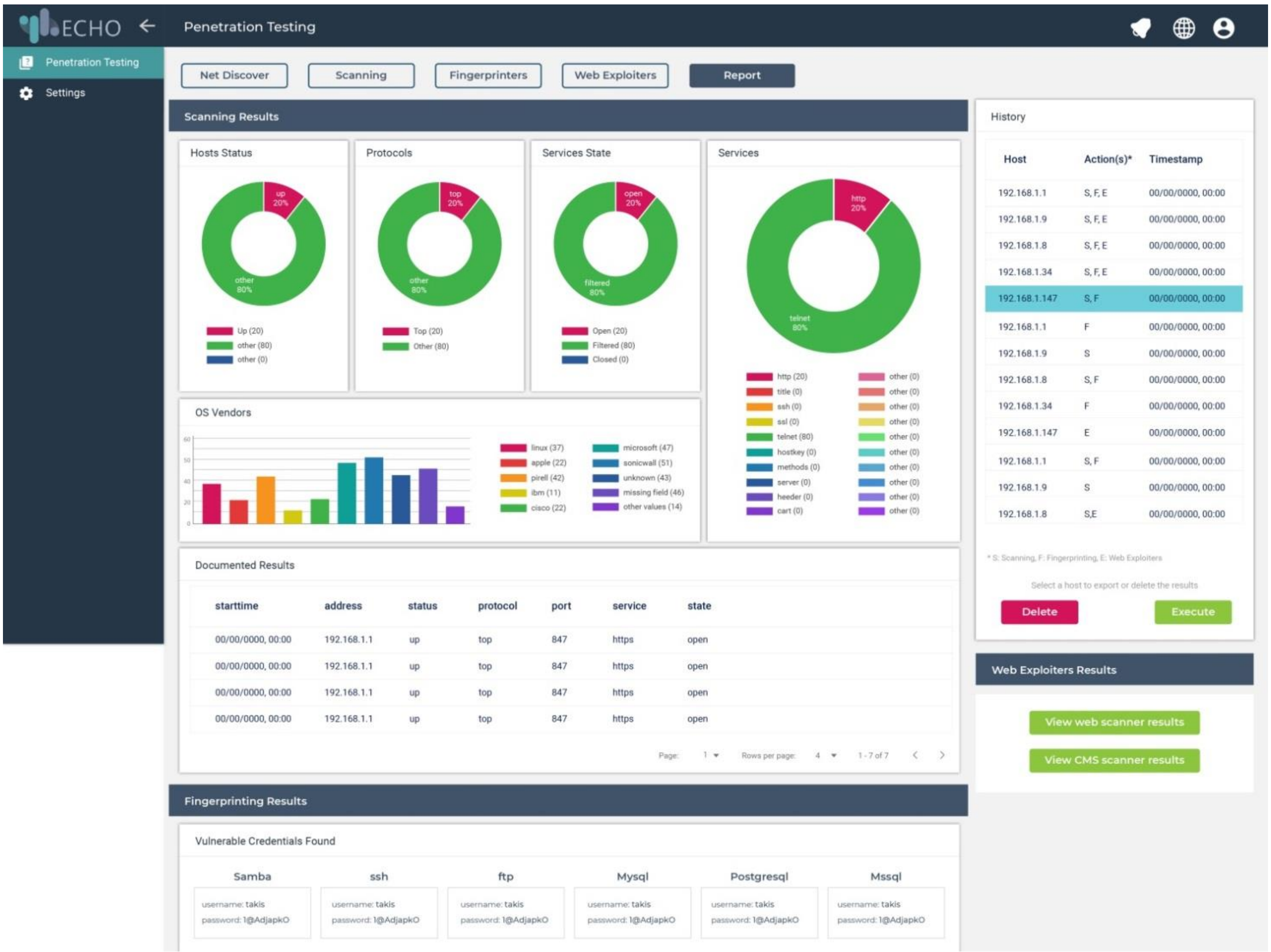
Attack Host *

192.168.1.1

Figure 4: Web Exploiters

Report

The final view of the Penetration Testing tool UI is the report, as depicted in Figure 5. The results from all the aforementioned views are visualized here to give the user a comprehensive view of the final report. Additionally, on the right corner of the view, a history table is shown, giving the user the ability to analyse reports from the past. Specifically, the user here can see the open ports and their services with potential exploits, if available. On the fingerprinting results, the user can see the credentials found during the fingerprinting phase. Lastly, on the web exploitation results, two buttons are provided with the results of each one of the Web Exploiters.



History

Host	Action(s)*	Timestamp
192.168.1.1	S, F, E	00/00/0000, 00:00
192.168.1.9	S, F, E	00/00/0000, 00:00
192.168.1.8	S, F, E	00/00/0000, 00:00
192.168.1.34	S, F, E	00/00/0000, 00:00
192.168.1.147	S, F	00/00/0000, 00:00
192.168.1.1	F	00/00/0000, 00:00
192.168.1.9	S	00/00/0000, 00:00
192.168.1.8	S, F	00/00/0000, 00:00
192.168.1.34	F	00/00/0000, 00:00
192.168.1.147	E	00/00/0000, 00:00
192.168.1.1	S, F	00/00/0000, 00:00
192.168.1.9	S	00/00/0000, 00:00
192.168.1.8	S,E	00/00/0000, 00:00

* S: Scanning, F: Fingerprinting, E: Web Exploiters

Select a host to export or delete the results

Web Exploiters Results

Documented Results

starttime	address	status	protocol	port	service	state
00/00/0000, 00:00	192.168.1.1	up	top	847	https	open
00/00/0000, 00:00	192.168.1.1	up	top	847	https	open
00/00/0000, 00:00	192.168.1.1	up	top	847	https	open
00/00/0000, 00:00	192.168.1.1	up	top	847	https	open

Fingerprinting Results

Vulnerable Credentials Found

Samba	ssh	ftp	Mysql	Postgresql	Mssql
username: takis password: 1@AdjapkO	username: takis password: 1@AdjapkO	username: takis password: 1@AdjapkO	username: takis password: 1@AdjapkO	username: takis password: 1@AdjapkO	username: takis password: 1@AdjapkO

Figure 5: Report

Description of the Tool Demo

The PT tool will be used by an attacker in order to attack in an intentional vulnerable machine. In general, PT will analyse any vulnerable machine provided in a Blue Team/Red Team exercise or even in a real-world scenario. For the needs of this demo the intentionally vulnerable machine has a Joomla content Management System (CMS) version 3.4.3 which is vulnerable to various known attacks and is hosted as a standalone virtual machine. Furthermore, the PT tool will be hosted in kali Linux virtual machine and will be used to attack and compromise the vulnerable machine. Thus, the local area network of the testbed consists of two virtual machines, the first is the machine that runs the tool and the second is the vulnerable machine.

In order to find the local IP address of the vulnerable machine the first **Net Discover** tab will be used. The local area network scan of the tool revealed two IP addresses the first is the IP address of the kali machine and the second is the IP address of the vulnerable machine.

The attacker then will use the second **scanning** tab in order to find an initial hole on the vulnerable machine. The PT tool gives the functionality to the attacker to select the port range and the time of the scan, the scan type and two scripts. Moreover, the attacker has the ability to run the **fingerprinting** and **web exploitation** tabs automated using the results of the scanning tab as input. The overall results of the PT tool will be presented to the user in the **report** tab.

The PT tool found four open ports 22, 80, 5000, 8081, 9001. In 22 port an OpenSSH service is running and in 80, 5000, 8081, 9001 a Nginx server is running on each of them with a Joomla CMS website. Furthermore, the vulners script used in the scan, suggests to the user various known vulnerabilities. Moreover, in the web exploiters tab the detected vulnerabilities and exploits are presented. The attacker then can test each one of the suggested vulnerabilities and exploits in order to check which one is working. Indeed, the attacker can test the most famous exploit for joomla 3.4.3 version suggested by the PT tool and may gain an initial meterpeter shell in the vulnerable machine. In order to attack in the vulnerable machine, the attacker can either run the exploit manually or can use the metasploit framework.

Tool related questions

Question #17.1.PTT

Did the Penetration Testing tool helped you identify accurately your network's topology?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Question #17.2.PTT

Did the PT tool helped you to scan for the open ports and services accurately?

Expected category of answer: **[choice]**

Option list for answer: **[Yes,** No]

If the user replies “No”, a new question appears

If No, in which way would you enhance this specific functionality of the tool?

Expected category of answer: **[textbox]**

Question #17.3.PTT

Did the PT tool helped you to find user credentials using the fingerprinters accurately?

Expected category of answer: **[choice]**

Option list for answer: **[Yes,** No]

Il the user replies “No”, a new question appears

If No, in which way would you enhance this specific functionality of the tool?

Expected category of answer: **[textbox]**

Question #17.4.PTT

Did the PT tool helped you to identify vulnerabilities on http services using the web exploiters tab accurately?

Expected category of answer: **[choice]**

Option list for answer: **[Yes,** No]

Il the user replies "No", a new question appears

If No, in which way would you enhance this specific functionality of the tool?

Expected category of answer: **[textbox]**

Question #17.5.PTT

Did the PT tool presented to you in a user-friendly report tab all the results accurately?

Expected category of answer: **[choice]**

Option list for answer: **[Yes,** No]

Il the user replies "No", a new question appears

If No, in which way would you enhance this specific functionality of the tool?

Expected category of answer: **[textbox]**

Question #17.6.PTT

In what capacity could the Penetration Testing tool replace the job of a penetration tester?

Expected category of answer: **[choice]**

Option list for answer: **[Scale 1-5]**

3.1.2 Trust & Quality Metrics

Description of the Tool

The idea behind defining trust and quality metrics for the threat intelligence data that is shared amongst EWS partners is to decrease the level of information overload as well as reduce false positives, which are both common in most cyber threat intelligence sharing platforms.

The TQM prototype aims to propose metrics to be used to rate the quality of threat intelligence data shared between partners, and by this, improve the trust in the relevancy of information shared among them. It will also enable an option to assess the trustworthiness of received information and its source based on metrics directly attributed to the trust level.

The incentive for the creation of the prototype is to:

- ✓ allow organisations to view automated evaluation of the quality of the information received;
- ✓ allow organisations to assess whether they can trust the organization sharing the information;
- ✓ help organisations to prioritise the information they should pay attention to.

Specific metrics defining Trustworthiness and Quality of threat intelligence data will be derived from the analysis described in D4.5 inter-sector prototypes. D4.5 describes as well the Implementation of metrics into the threat intelligence data-sharing platform.

Capabilities

A list of the basic tool's capabilities is shown in the following table.

Category	Functionality	Description
Quality of Threat Intelligence	**Give a quality score to threat intelligence**	A quality score will be given to the threat intelligence that partners have shared within their constituents. This will help them in identifying which threat intelligence is relevant for their purposes. Also, the quality score will affect the trustworthiness level of the partner based on retroactive sharing activity, which could potentially be another metric used to establish trust between partners.
Trust between Partners	**Give a trustworthiness score to partners**	A Trust score will be given to each partner producing CTI based on pre-defined metrics. One example of a metric could be whether or not the partner who shared the threat intelligence is within the same constituent as the partner who is viewing it.
Reputation of Partner	**Give an overall trust score of a partner**	A Reputation score will be given to a partner considering the Trust scores computed by each instance of the Trust and Quality Metric Prototype.

Table 5: Capabilities of the Trust & Quality Metrics tool

Description of the Tool Demo

The research and development done behind the Trust and Quality Metrics (TQM) prototype aims to help users of information-sharing platforms to navigate through the amount of Cybersecurity Threat Intelligence (CTI) and identify the information of the highest quality, the most relevant to their organisation, shared by the most trustworthy sources. Apart from predefined quality and trust metrics and algorithms for their calculation, the user will be given an option to personalise their own preferences and priority areas. Currently, the tool is under development, with the planned release of version 2 in January 2022. Due to its character, its value-added can be best demonstrated in conjunction with E-EWS demonstrations in spring 2022. The devoted site on the ECHO website will also include a small demonstration of TQM's application in the form of slide-deck or short video.

Tool related questions

Question #17.1.TQM

***Would you take into consideration the automatic evaluation of CTI's quality when assessing it?* Select all that applies. If you see other benefits or concerns, please share them in the "other" textbox**

Expected category of answer: **[multiple choice]**

Option list for answer: **[***I find this option helpful to prioritise the information*
I would use it, only If I can verify the evaluation logic and will agree with it
I would use it, only if I can customize the quality criteria (define which metric should be given how much importance)
It could lead us to overlooking important intel
*Other [textbox]]***

If the user selects "Other", a new textbox appears for further clarification.

Expected category of answer: **[textbox]**

The rationale of this question is to confirm the demand and usability of this algorithm.

Question #17.2.TQM

Would you take into consideration the automatic evaluation of the trustworthiness of the source sharing this information? Select all that applies. If you see other benefits or concerns, please share them in the "other" textbox

Expected category of answer: **[multiple choice and/or textbox]**

Option list for answer: **[** *I find this option helpful to prioritize the information*
I would use it, only If I can verify the evaluation logic and will agree with it

I would use it, only if I can customize the trust criteria (define which metric should be given how much importance)
it could lead us to overlook some important intel
Other [textbox]]

If the user selects “Other”, a new textbox appears for further clarification.

Expected category of answer: **[textbox]**

The rationale of this question is to confirm the demand and usability of this algorithm.

3.1.3 CVE Strainer

Description of the Tool

The CVE-Strainer stand-alone platform is designed to overcome the above-mentioned challenges (and address challenges identified in ECHO T4.1) and may be used to timely push the notifications to its users for the specified devices of the infrastructure.

The high-level concept of the CVE-Strainer, shown in Figure 6, can be described as:

1. A CMDB is either imported; information for systems, corresponding vendors and exact versions is entered manually or is updated into the CVE-Strainer’s device database.
2. Periodical queries for vulnerabilities are executed towards (the list is not exhaustive and may be expanded):
   a. NVD to gather data for new CVEs, CPEs, CWEs and CAPEC items.
   b. Exploit Database.
   c. Local database.
3. Periodical queries, based on API calls and custom parsers, for vendor patches and updates, are executed towards (the list is not exhaustive and does not contain all monitored vendors):
   a. Microsoft security bulletins.
   b. Apple security updates.
   c. Cisco security advisory.
   d. Local database.
4. The records in the device database are verified for newly discovered vulnerabilities and patches and if new correlations are discovered a notification is pushed to predefined users in the pre-configured format: email, mobile push notification, etc.

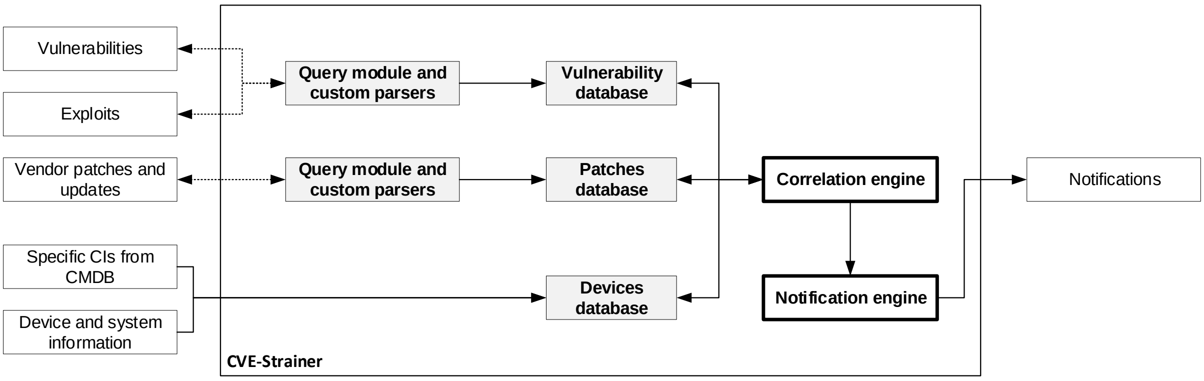


Figure 6: Overview of the CVE Strainer

The CVE Strainer design is modular, providing the expected level of flexibility, future extension, and performance.

By providing easy access and push notifications of the necessary information CVE Strainer addresses a variety of challenges identified in T4.1, achieving a key goal towards the selection of early prototype tools.

The tool is designed in such a way that it can be used in stand-alone configuration with little or no integration with other systems, as well as integrated via API.

Note that as part of the name of the tool contains “CVE”, it is important to note that the functionality is not limited to this type of data only. The initial idea for the system was based on NVD but was later extended to the current state (multiple exploit data sources and vendors).

Capabilities

A list of the basic tool’s capabilities is shown in the following table.

Category	Functionality	Description	Note
Query module and custom parsers	**Information gathering and parsing**	Performs API calls, online database access and website searches to gather information for the latest: • CVE • Exploits • Vulnerabilities • Patches and updates • Etc. The data is parsed and stored in the CVE-Strainer’s databases in a common format.	
Vulnerability database	**Data storage and querying**	Stores and indexes information regarding the latest CVEs, exploits and vulnerabilities.	

Category	Functionality	Description	Note
Patches database	**Data storage and querying**	Stores and indexes information regarding the latest patches and updates for various vendors.	
Devices database	**Data storage and querying**	Stores and indexes information regarding the devices in the user's infrastructure.	
Correlation engine	**Data analysis**	Performs analysis of the information in vulnerability database, patches database and correlates the data to the records in the devices database. For any new findings, a message to the notification engine is sent.	
Notification engine	**Notification**	Summarizes the results from the correlation engine and pushes notifications to predefined points of contact by email, mobile notification, etc.	

Table 6: Capabilities of the CVE Strainer tool

Description of the Tool Demo

Onboarding the tool requires a dedicated host with minimal system requirements. A CMDB or a similar list of assets containing products and their versions, formatted in a way that is supported by the tool, is necessary for the tool to operate. Additionally, that list should also include a client_id variable (such as the client's name), in order to uniquely identify these assets as being owned by the specific client. Furthermore, the client_id variable should also be configured in the tool's database alongside an e-mail address. This e-mail address will be used as the recipient for all findings pertaining to the specific client's assets, as configured by the CMDB/asset list.

Once the initial CMDB and client configurations are complete, the tool's message broker should be started using the docker container. Following that, the tool's Parser Module, Database Module, Correlation Module and Notification Module can be started. Once all listeners are active and awaiting data, the Query module can be started, which also begins the cycle of periodic querying, and data parsing when required.

The tool will continue working until stopped and will notify the configured client by an e-mail when a new vulnerability or patch is discovered that is affecting their configured assets.

Tool related questions

Question #17.1.CVE_S

Was the information contained in CVE-Strainer's automatically generated notification sufficient in handling the discovered vulnerability and/or patch?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

This question is relevant due to the wide array of information contained in both vulnerabilities and patches. The goal of CVE-Strainer is to not only provide accurate and timely notifications, but also to ensure their applicability.

Question #17.2.CVE_S

What other sources of information pertaining to vulnerabilities and patches would be critical to include in the tool's functionality in order to facilitate a wider adoption in production environments?

Expected category of answer: **[textbox]**

The tool's array of supported vulnerability/patch sources is constantly evolving and should be supplemented in a way that furthers the goal of optimal adoption.

3.1.4 CyMS's HMI

Description of the Tool

CyMS is software produced by Naval Group and aims to foster the Cyber Defence of an IT/OT infrastructure onboard ships. With its two main functionalities: cyber supervision and administration, it enables the operator's awareness of relevant cyber threats and suggests mitigation actions to contain the attack. It collects logs from heterogeneous distributed sensors, processes datasets, raises value-added alarms and manages cyber incidents.

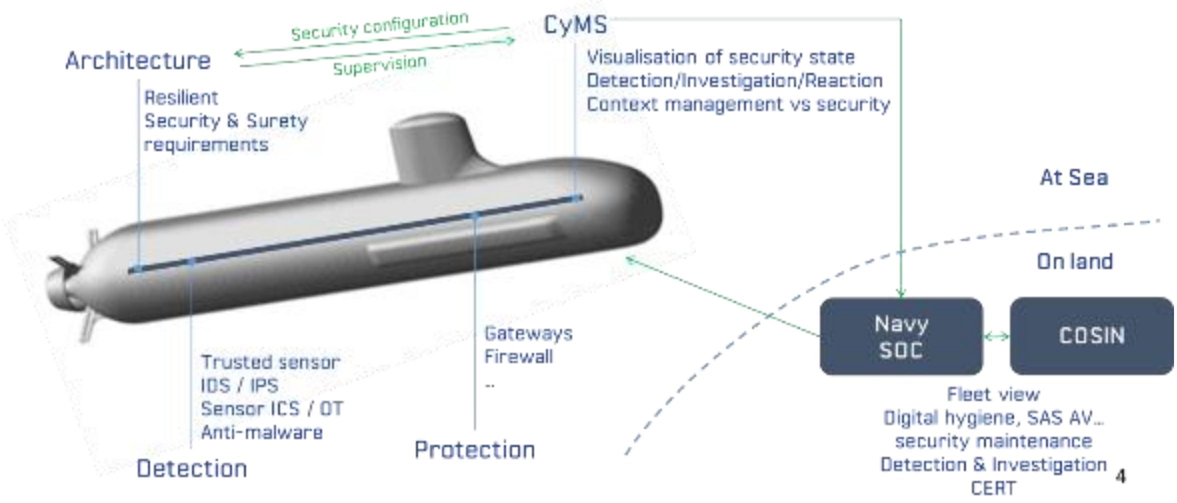


Figure 7: CyMS Big Picture

Within the ECHO project and the WP4, the concept is going to be extended by developing a new Human Machine Interface (HMI). This interface will be dedicated to responding to the challenge of the presentation of a cyber complex situation to crew members who are not cyber experts. It offers an answer mainly to the challenge ID16: Lack of dedicated tools to manage Cyber Threats, identified in T4.1.

In more details, the concept developed will try to give a synthetic view of cyber threats which hamper the main critical functions of a ship or a system.

Capabilities

A list of the basic tool's capabilities is shown in the following table.

Category	Functionality	Description	Note
Human Machine Interface	**Presentation of relevant information to unskilled users**	Centralizes all security information Focuses on high-level security incidents Makes a security incident understandable by a non-expert Empowers the operator on board to adopt the best reaction regarding the incident and the operational context	

Table 7: Capabilities of the CyMS Tool

Description of the Tool Demo

CyMS HMI will be hosted in a Linux based machine reachable over a private network inside the NG cyberange. The CyMS IHM tool is the main topic of the 2 demo cases. However, it should be noted that CyMS IHM will be implemented in two different ways.

In the first demo case, CyMS IHM will be the focus of an evaluation carried out by an external operator in order to check his builtin security capabilities.

None of its SIEM/SOAR features will be demonstrated at this time. The overall posture of the tool will be rather passive. Different security requirements will be checked by an auditor in accordance of a Security Target. The auditor will connect to CyMS HMI from a separate external cyberange. The security requirements that will be assessed are grouped into the following families:

- Security Audit- Identification and Authentication
- Security Management
- Access Control
- Trusted path/channels

In order to ensure a good level of assurance of the assessment, a vulnerability analysis will be performed. To help the auditor in his approach, a specific VM hosting different security tools will be provided. The Vulnerability Analysis will help to complete the certification report.

The second demo will show the regular use of the tool in a more active way. CyMS HMI will be hosted inside the NG cyberange with a VM including a vulnerability scanner. This scanner will be connected to an OT network hosted in an external cyberange and will feed CyMS IHM with new unknown logs. The R&D approach will consist to allow CyMS to handle these new logs in order to improve the comprehension skills of the operators and assist them to adopt the best reaction if the sudden discovery of a vulnerability occurs.

To achieve this, a specific user account will be created (**ECHO-CyMS-HMI-FNC-0060**) and then used to authenticate on CyMS IHM (**ECHO-CyMS-HMI-FNC-0010**). The operator will initiate a vulnerability scan on the target network using the Portal (**ECHO-CyMS-HMI-FNC-0070**) and will be able to list the vulnerabilities found from the dashboard (**ECHO-CyMS-HMI-FNC-0020**). Therefore, the operator will be able to handle the appropriate reactions (**ECHO-CyMS-HMI-FNC-0040**, **ECHO-CyMS-HMI-FNC-0050**)

Tool related questions

Question #17.1.CyMS

In your opinion, on a scale of 1 to 5 (1 being the worst and 5 the best), do you feel that the use of the CyMS HMI allows a user with low Cyber skills to effectively become aware of a Cyber event and to react autonomously and correctly to the displayed threat?

Expected category of answer: **[choice]**

Option list for answer: **[scale 1-5]**

This question is relevant due to the complexity and the amount of information contained in log entries but also the difficulty of linking technical facts to high level ship functions.

Question #17.2.CyMS

What additional features/approach would improve the function of presenting relevant information to unskilled users? How can the decision-making process be simplified?

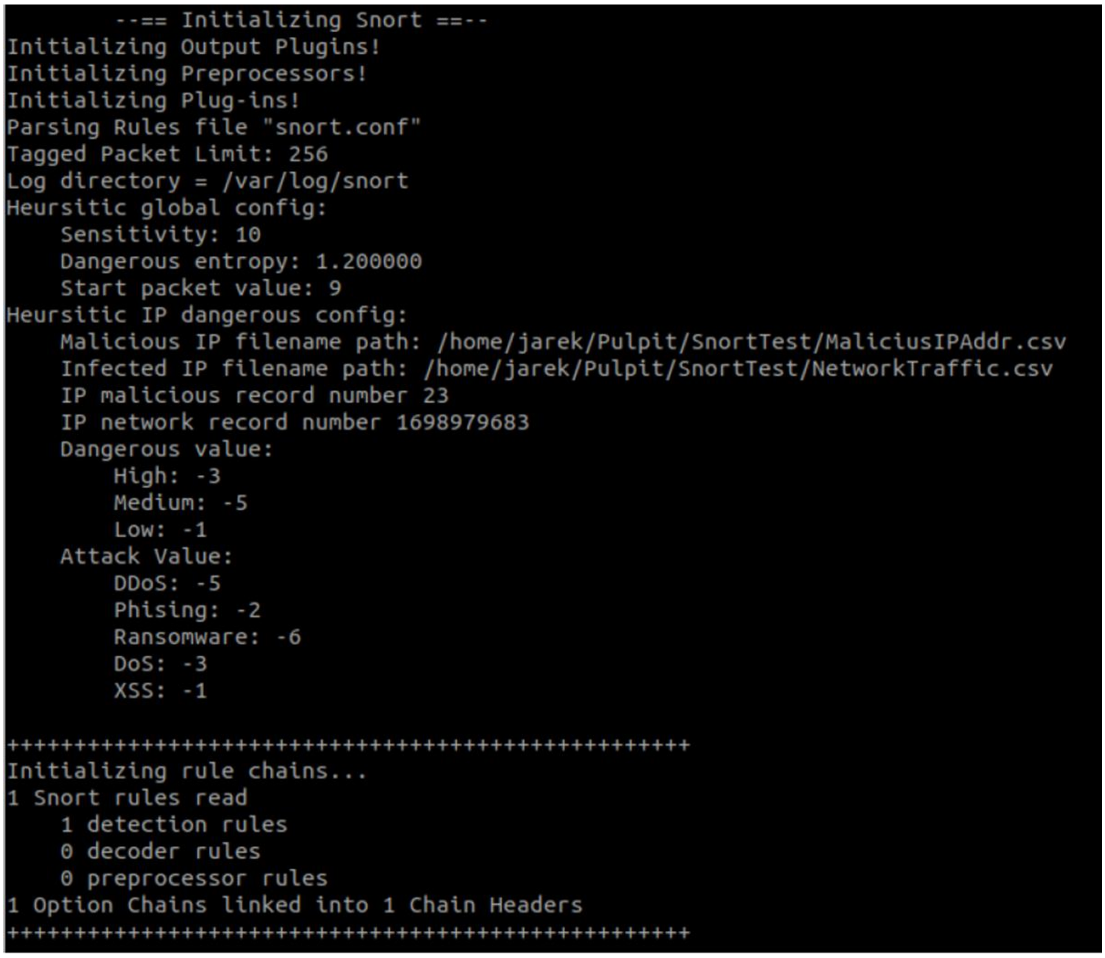
Expected category of answer: **[textbox]**

This question is relevant because complexity only increases and operators have to decide on the most appropriate corrective actions more and more quickly.

3.1.5 SNORT module

The SNORT module is based on Snort environment, however contains extended functionality – heuristic approach to intrusion detection based on external data. Snort as an environment is a free open source Network Intrusion Detection System (NIDS) capable of logging and/or analysing incoming traffic in real-time on IP networks. It was originally released in 1998 as a cross-platform network sniffing tool. With the help of the community members, it evolved into a powerful Intrusion Detection and Prevention System (IDS/IPS). It is a great example of how successful an open-source tool can be, when developed in cooperation with the users, for example by reporting and even fixing bugs or contributing to the source code. The tool itself is free, but it is based on a paid subscription model – the newest threat rules are available for those who subscribed immediately, while free users get access to rules after 30 days. However, the Open Source model of Snort engine allows us to increase the functionality of intrusion detection using heuristic algorithms.

During the activities of T4.3 we implemented new functionality in Snort environment to address selected cybersecurity challenges, defined in T4.1. This work will be focused on the development of selected modules of Snort engine – mainly preprocessors. The development of the SNORT module extends the functionality of Snort environment by a heuristic approach to intrusion detection and external data from third parties (e.g. federation of entities in a specific sector). The functionality has been designed in such a way that the user, through configuration, can influence the operation of the detection algorithm. To implement the algorithm, new pre-processors have been added to the Snort environment. Snort engine consists of a sniffer (packet acquisitor and decoder), preprocessors, detection engine, and the output responsible for generating alerts. The crucial element of Snort architecture allowing to implementation of new functionalities is the preprocessor. The main work towards SNORT module implementation was focused on this element (e.g. such functions as HeuristicDetectionGlobalInit, HeuristicDefaultValue, HeuristicParseGlobalArgs, and others). SNORT module operates using a console and configuration is based on data in text files, e.g. snort.conf (console view when SNORT module is started presented in Figure 8).



```
        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "snort.conf"
Tagged Packet Limit: 256
Log directory = /var/log/snort
Heursitic global config:
    Sensitivity: 10
    Dangerous entropy: 1.200000
    Start packet value: 9
Heursitic IP dangerous config:
    Malicious IP filename path: /home/jarek/Pulpit/SnortTest/MaliciusIPAddr.csv
    Infected IP filename path: /home/jarek/Pulpit/SnortTest/NetworkTraffic.csv
    IP malicious record number 23
    IP network record number 1698979683
    Dangerous value:
        High: -3
        Medium: -5
        Low: -1
    Attack Value:
        DDoS: -5
        Phising: -2
        Ransomware: -6
        DoS: -3
        XSS: -1

+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
1 Snort rules read
    1 detection rules
    0 decoder rules
    0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++
```

Figure 8: SNORT module – console view of the started application

The algorithm starts with creating a file or receiving a file saved in Comma-Separated Values (CSV) format. The file contains malicious IP address, several flags, and entropy value. Such file can be provided by another company from a federation that was attacked and after forensic analysis. Flags with their default values are described below.

- **dangerous** – This flag identifies the severity of the threat associated with an IP address (e.g. High, Medium and Low). The value of this flag is subjective and depends on the environment in which the preprocessor is used. In some cases, the attack will not do much harm, e.g. a phishing attack on medical wristband infrastructure will not do much harm, but instead, the same type of attack on a corporate infrastructure can do great harm. The value of this flag and the decision on which flag to assign to the given IP address can be based on the analysis of other flags.
- **attack** – This flag specifies the type of attack in which the IP address was recently involved (e.g. Phishing, DDoS, Ransomware, XSS, etc.). The value of this flag may differ from the environment because the effectiveness of an attack also depends on the purpose of the network and who is using it.
- **range** – This type of flag describes the impact of an attack by an IP address on other network components such as a server, a switch or a router. In this case, a given attack may affect only a single attacked network component or spread over a part or all of the infrastructure.

- **access** – Some attacks (e.g. phishing, malware) require user action within the network, others (e.g. DDoS, DoS) do not require user intervention. This type of flag describes the need for user activity within the network. For example, we can define two possible flags: none and user. The first describes the situation when an attack does not need the user's activity. The second describes the situation when an attack needs a user's activity (e.g. opening an attachment in an email).
- **availability** – Some attacks, such as ransomware, cause partial or complete loss of access to the unit and data on it. This type of flag describes the impact on the availability of the attacked component. For example, we can define three levels of impact on the functionality of a given component in network: (1) Attack does not affect the functionality of the station, (2) Attack causes the loss of several functionalities and a decrease in performance, (3) Attack causes a complete loss of control of the unit.

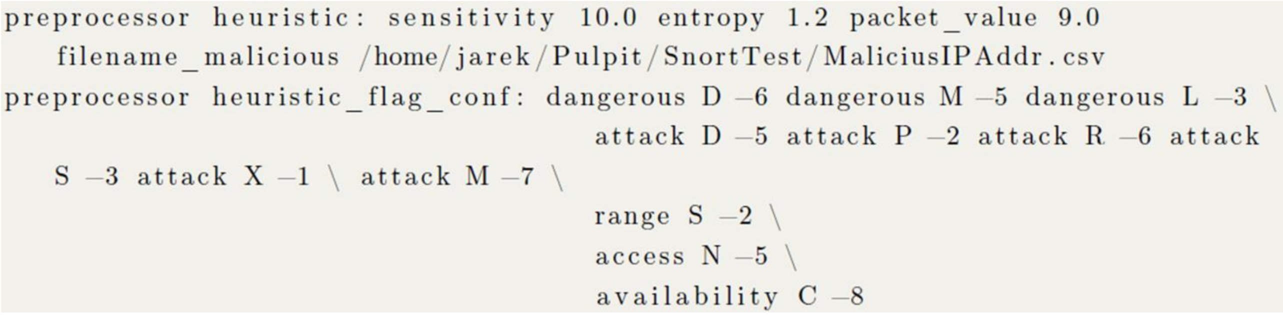
Description of the Tool Demo

Snort can be configured to work as a NIDS. In this module, Snort is reading a configuration file (snort.conf) and looks for 'Snort rules'. The configuration file should indicate the options of a new heuristic preprocessor. The first preprocessor (heuristic) is a master preprocessor, which means it must be in the configuration file if it is to be used to detect attacks. The options that can be configured are:

- **sensitivity** – the lower limit of the packet value (when this limit is exceeded, the package is reported to the console);
- **entropy** – the upper limit of the packet entropy value (above which the packet is reported to the console);
- **packet_value** – the base value of the packet, (which is received immediately after delivering the packet to the preprocessor (this value is the same for every packet that is analysed)).

The second preprocessor, called heuristic_flag_conf, is dependent on the main preprocessor. It cannot be used if the main preprocessor is not enabled. The subordinate preprocessor is mainly used to configure the values of individual flags. As in the case of the master preprocessor, if the flag value is not changed, the detection will take into account the default value.

In Figure 9 the configuration file with new preprocessors is presented.



```
preprocessor heuristic: sensitivity 10.0 entropy 1.2 packet_value 9.0
   filename_malicious /home/jarek/Pulpit/SnortTest/MaliciusIPAddr.csv
preprocessor heuristic_flag_conf: dangerous D -6 dangerous M -5 dangerous L -3 \
                                  attack D -5 attack P -2 attack R -6 attack
   S -3 attack X -1 \ attack M -7 \
                                  range S -2 \
                                  access N -5 \
                                  availability C -8
```

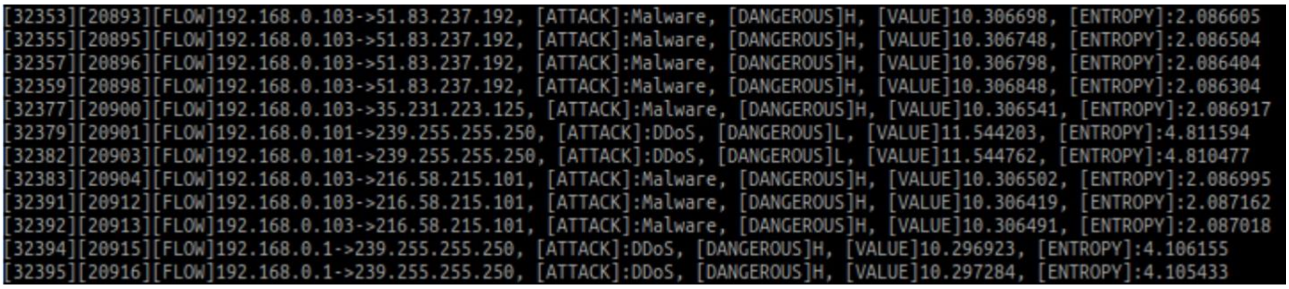
Figure 9: Configuration file with heuristic preprocessor

The final value of the packet should depend on the value of each flag in the appropriate proportion and the entropy. In the case of a dangerous and attack flag, it is a subjective assessment of how to evaluate the attack. For example, we can assume 65% of the dangerous flag value and 35% of the attack flag value for the final decision (together gives 100%). We can also limit the influence of the entropy value if needed (e.g. 50%

of entropy value for a given IP address). The final formula for calculating the final packet value can be as following:

*Initial_packet_value + (0.65 * dangerous) + (0.35 * attack) + range + access + availability + (0.5 * entropy)*

However, the final decision of packet value must be compliant with the assumed security policy for a given network/system. Therefore, these coefficients should be personalized. An example of received logs which indicates that malicious network traffic occurred at network interface is presented in Figure 10.



```
[32353][20893][FLOW]192.168.0.103->51.83.237.192, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306698, [ENTROPY]:2.086605
[32355][20895][FLOW]192.168.0.103->51.83.237.192, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306748, [ENTROPY]:2.086504
[32357][20896][FLOW]192.168.0.103->51.83.237.192, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306798, [ENTROPY]:2.086404
[32359][20898][FLOW]192.168.0.103->51.83.237.192, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306848, [ENTROPY]:2.086304
[32377][20900][FLOW]192.168.0.103->35.231.223.125, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306541, [ENTROPY]:2.086917
[32379][20901][FLOW]192.168.0.101->239.255.255.250, [ATTACK]:DDoS, [DANGEROUS]L, [VALUE]11.544203, [ENTROPY]:4.811594
[32382][20903][FLOW]192.168.0.101->239.255.255.250, [ATTACK]:DDoS, [DANGEROUS]L, [VALUE]11.544762, [ENTROPY]:4.810477
[32383][20904][FLOW]192.168.0.103->216.58.215.101, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306502, [ENTROPY]:2.086995
[32391][20912][FLOW]192.168.0.103->216.58.215.101, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306419, [ENTROPY]:2.087162
[32392][20913][FLOW]192.168.0.103->216.58.215.101, [ATTACK]:Malware, [DANGEROUS]H, [VALUE]10.306491, [ENTROPY]:2.087018
[32394][20915][FLOW]192.168.0.1->239.255.255.250, [ATTACK]:DDoS, [DANGEROUS]H, [VALUE]10.296923, [ENTROPY]:4.106155
[32395][20916][FLOW]192.168.0.1->239.255.255.250, [ATTACK]:DDoS, [DANGEROUS]H, [VALUE]10.297284, [ENTROPY]:4.105433
```

Figure 10: SNORT module – example of received logs (alerts)

Tool related questions

Question #17.1.SNORT

Which additional external information regarding a threat/an attack should be taken into account by the heuristic detection algorithm implemented in SNORT module?”

Expected category of answer: **[textbox]**

Any participant will be able to write a suggestion which external data (shared in a federation/sector) should be taken into account by heuristic intrusion detection algorithm.

Question #17.2.SNORT

Which sector can be the most appropriate to implement SNORT module?

Expected category of answer: **[textbox]**

The open question or participants can choose selected answers from the list of sectors. The question aims to indicate the most proper sectors for the prototype.

3.1.6 CTI Extractor

Description of the Tool

CTI extractor is a module that aims at the extraction, analysis and correlation of CTI from internal sources. Such sources include, but are not limited to, web services, databases, computer systems, and application logs.

Data collection and analysis targets concerning the acquisition of Indicators of Compromise (IoC):

- Hash Values
- IP Addresses
- Domain Names
- Network/Host Artifacts
- Tools
- TTPs

The aforementioned IoCs may eventually lead to CTI Information resulting from data gathering and analysis which needs to be converted into an actionable data format that can be digested by a machine and can be easily shared. Therefore, CTI is stored in a standardized format according to standards such as STIX2. Furthermore, applications regarding the calculation of the quality and trust of the CTI could benefit from avoiding unnecessary pre-processing.

Capabilities

A list of the basic tool's capabilities is shown in the following table.

Category	Functionality	Description	Note
Logs aggregation	**Aggregate logs from several internal sources**	The module will support the collection and aggregation of data from several internal sources	
Threat detection	**Detect threats using rule-based and machine learning-based methods**	The module will support the detection of threats by combining pre-defined rules as well as by using machine learning models to identify anomalies	
Attacks correlation	**Correlate attacks**	The module will support the correlation of attacks considering the adversaries' tactics, techniques, and procedures	

Category	Functionality	Description	Note
CTI extraction	**Extraction of CTI**	The module will support the extraction of the CTI in a standardised format	

Table 8: Capabilities of the CTI Extractor tool

High-Level Structure View

A basic architecture view of the tool, as described, is depicted in the following figure.

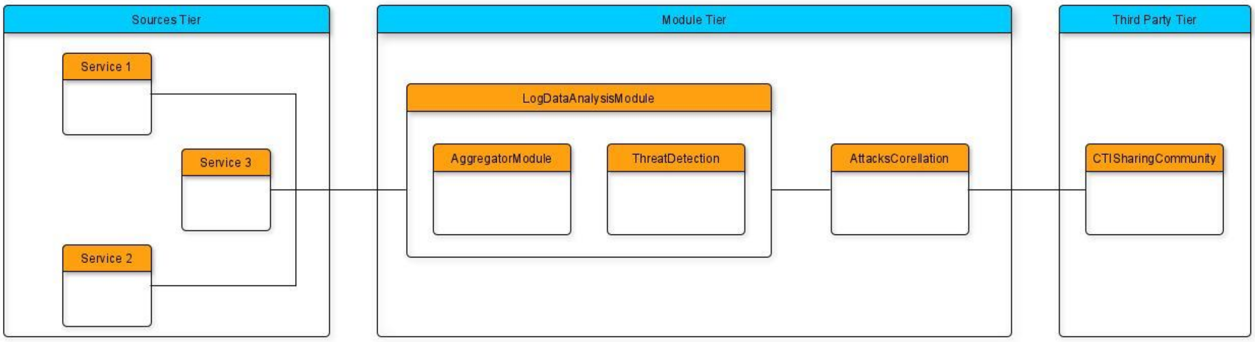
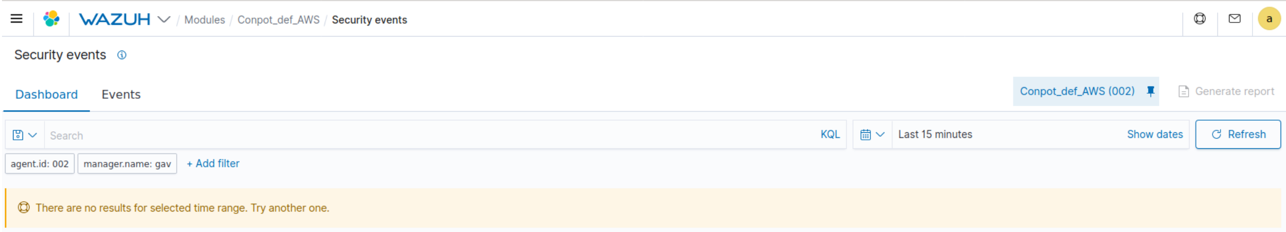


Figure 11: CTI Extractor tool – Structural architecture

User interface/Mockups

CTI Extractor utilises a Wazuh instance for the analysis of the logs from internal sources and the detection of security alerts. The Wazu instances have been enriched with custom decoders and rules to cover a wider range of cyber-attacks, including Industrial Control Systems (ICS) attacks such as Modbus and Guardian AST. Furthermore, the instance will be configured to meet further needs of the CTI Extractor.

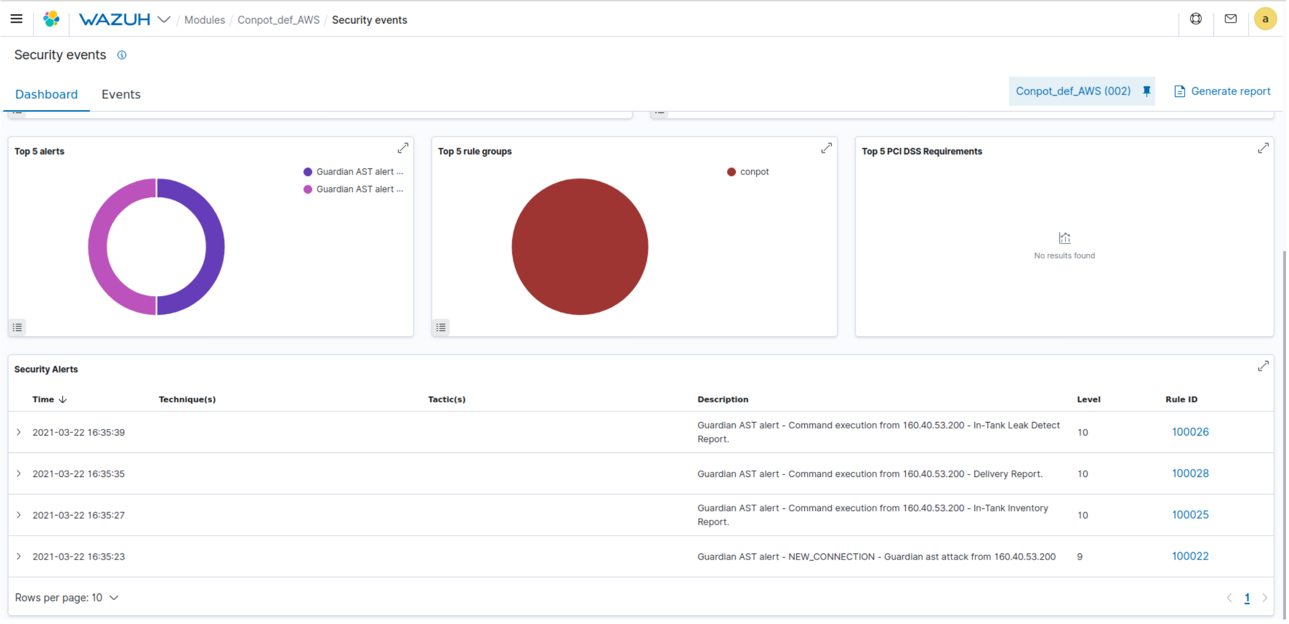
The following Figures Figure 12-Figure 16 are screenshots of the Wazuh dashboard and show the detection capabilities of CTI Extractor using custom detection rules. The figures depict the detected security incidents that occurred during the last 15 minutes.



There are no results for selected time range. Try another one.

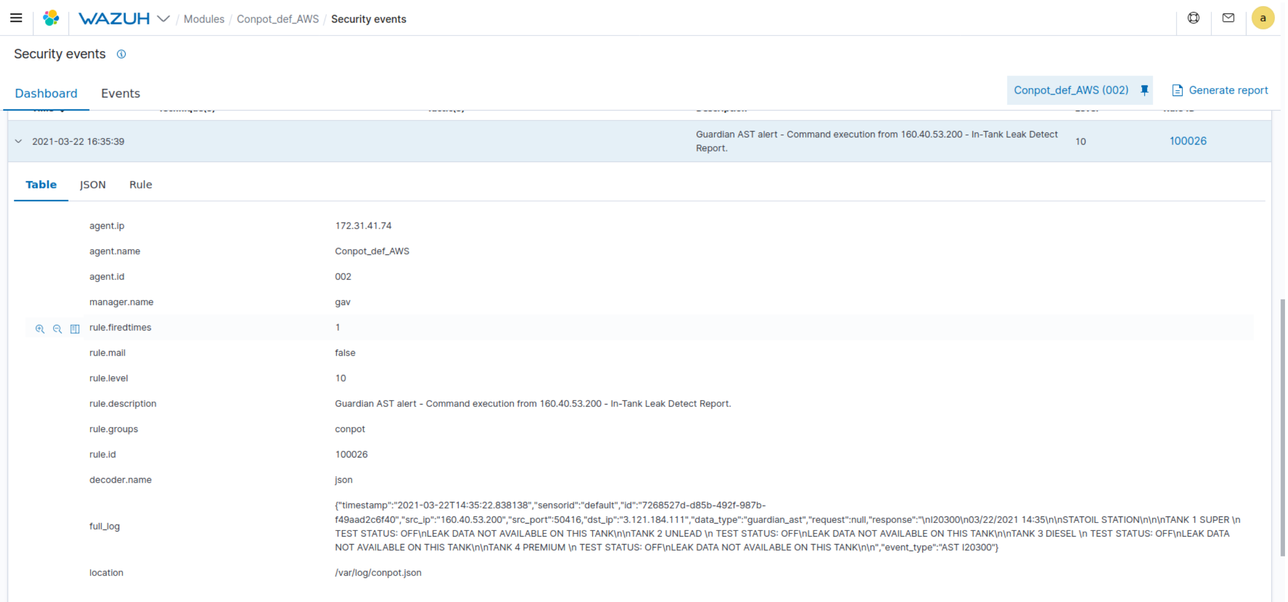
Figure 12: Wazuh dashboard

The attacker executes a set of TLS-350 commands which target Guardian AST monitoring systems. Given that the respective rules have been developed, the attacks are detected and listed on the dashboard.



Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
2021-03-22 16:35:39			Guardian AST alert - Command execution from 160.40.53.200 - In-Tank Leak Detect Report.	10	100026
2021-03-22 16:35:35			Guardian AST alert - Command execution from 160.40.53.200 - Delivery Report.	10	100028
2021-03-22 16:35:27			Guardian AST alert - Command execution from 160.40.53.200 - In-Tank Inventory Report.	10	100025
2021-03-22 16:35:23			Guardian AST alert - NEW_CONNECTION - Guardian ast attack from 160.40.53.200	9	100022

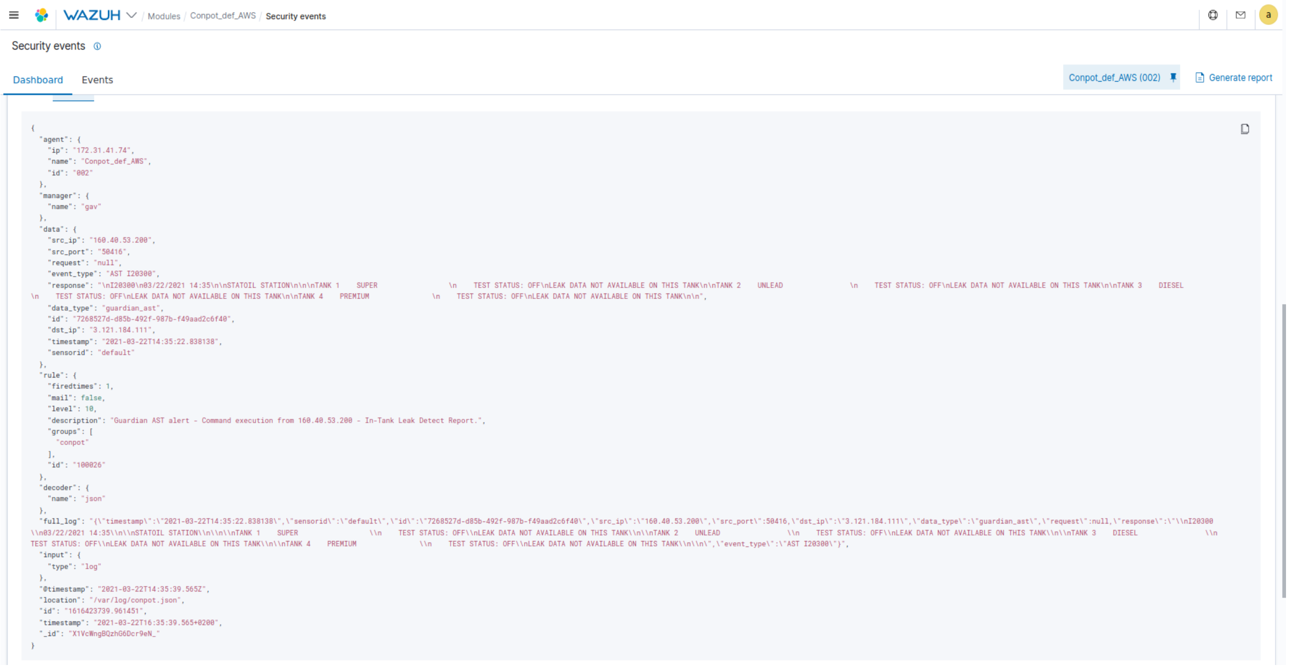
Figure 13: Detected security incidents (new connection, I20100, I20200, I20300)



2021-03-22 16:35:39 Guardian AST alert - Command execution from 160.40.53.200 - In-Tank Leak Detect Report. 10 100026

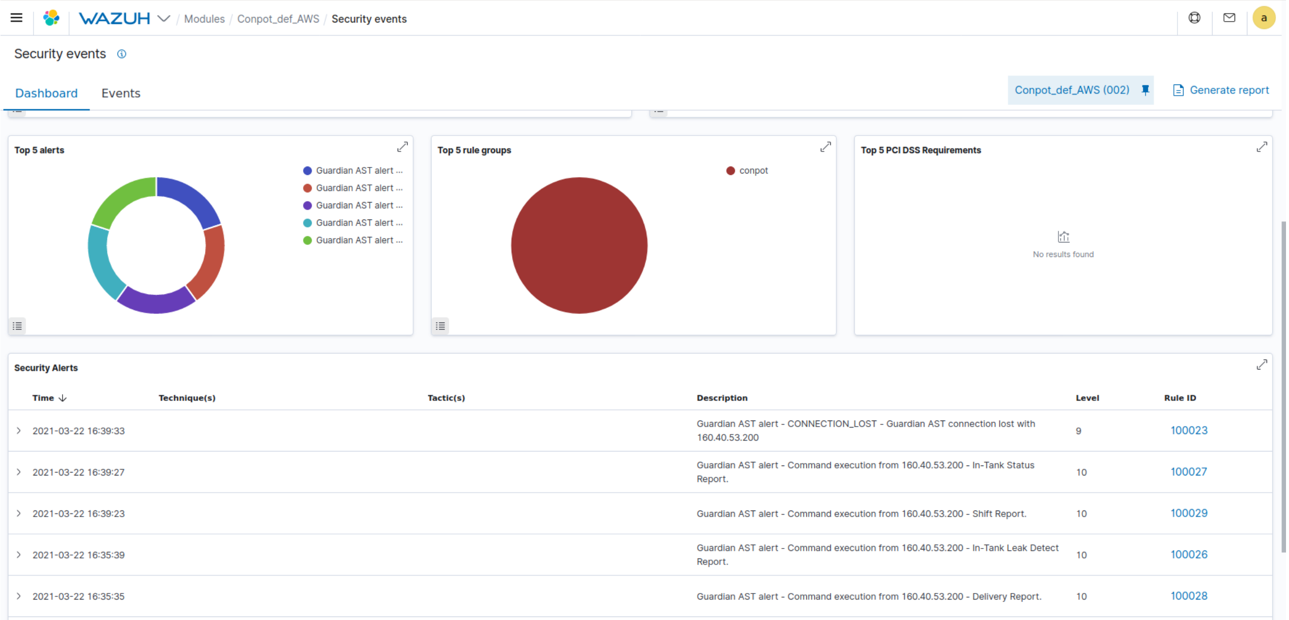
agent.ip	172.31.41.74
agent.name	Conpot_def_AWS
agent.id	002
manager.name	gav
rule.firedtimes	1
rule.mail	false
rule.level	10
rule.description	Guardian AST alert - Command execution from 160.40.53.200 - In-Tank Leak Detect Report.
rule.groups	conpot
rule.id	100026
decoder.name	json
full_log	{"timestamp":"2021-03-22T14:35:22.838138","sensorid":"default","id":"7268527d-d85b-492f-987b-f49aad2c6f40","src_ip":"160.40.53.200","src_port":50416,"dst_ip":"3.121.184.111","data_type":"guardian_ast","request":null,"response":"\nI20300\n03/22/2021 14:35\n\nSTATOIL STATION\n\n\nTANK 1 SUPER \n TEST STATUS: OFF\nLEAK DATA NOT AVAILABLE ON THIS TANK\n\nTANK 2 UNLEAD \n TEST STATUS: OFF\nLEAK DATA NOT AVAILABLE ON THIS TANK\n\nTANK 3 DIESEL \n TEST STATUS: OFF\nLEAK DATA NOT AVAILABLE ON THIS TANK\n\nTANK 4 PREMIUM \n TEST STATUS: OFF\nLEAK DATA NOT AVAILABLE ON THIS TANK\n\n","event_type":"AST I20300"}
location	/var/log/conpot.json

Figure 14: Security alert details



```
{
  "agent": {
    "ip": "172.31.41.74",
    "name": "Conpot_def_AWS",
    "id": "002"
  },
  "manager": {
    "name": "gav"
  },
  "data": {
    "src_ip": "160.40.53.200",
    "src_port": "50416",
    "request": "null",
    "event_type": "AST I20300",
    "response": "\nI20300\n03/22/2021 14:35\n\nSTATOIL STATION\n\n\nTANK 1    SUPER                  \n    TEST STATUS: OFF\nLEAK DATA NOT AVAILABLE ON THIS TANK\n\nTANK 2    UNLEAD                 \n    TEST STATUS: OFF\nLEAK DATA NOT AVAILABLE ON THIS TANK\n\nTANK 3    DIESEL
\n    TEST STATUS: OFF\nLEAK DATA NOT AVAILABLE ON THIS TANK\n\nTANK 4    PREMIUM                \n    TEST STATUS: OFF\nLEAK DATA NOT AVAILABLE ON THIS TANK\n\n",
    "data_type": "guardian_ast",
    "id": "7268527d-d85b-492f-987b-f49aad2c6f40",
    "dst_ip": "3.121.184.111",
    "timestamp": "2021-03-22T14:35:22.838138",
    "sensorid": "default"
  },
  "rule": {
    "firedtimes": 1,
    "mail": false,
    "level": 10,
    "description": "Guardian AST alert - Command execution from 160.40.53.200 - In-Tank Leak Detect Report.",
    "groups": [
      "conpot"
    ],
    "id": "100026"
  },
  "decoder": {
    "name": "json"
  },
  "full_log": "{\"timestamp\":\"2021-03-22T14:35:22.838138\",\"sensorid\":\"default\",\"id\":\"7268527d-d85b-492f-987b-f49aad2c6f40\",\"src_ip\":\"160.40.53.200\",\"src_port\":50416,\"dst_ip\":\"3.121.184.111\",\"data_type\":\"guardian_ast\",\"request\":null,\"response\":\"\\nI20300
\\n03/22/2021 14:35\\n\\nSTATOIL STATION\\n\\n\\nTANK 1    SUPER                  \\n    TEST STATUS: OFF\\nLEAK DATA NOT AVAILABLE ON THIS TANK\\n\\nTANK 2    UNLEAD                 \\n    TEST STATUS: OFF\\nLEAK DATA NOT AVAILABLE ON THIS TANK\\n\\nTANK 3    DIESEL                 \\n
TEST STATUS: OFF\\nLEAK DATA NOT AVAILABLE ON THIS TANK\\n\\nTANK 4    PREMIUM                \\n    TEST STATUS: OFF\\nLEAK DATA NOT AVAILABLE ON THIS TANK\\n\\n\",\"event_type\":\"AST I20300\"}",
  "input": {
    "type": "log"
  },
  "@timestamp": "2021-03-22T14:35:39.565Z",
  "location": "/var/log/conpot.json",
  "id": "1616423739.961451",
  "timestamp": "2021-03-22T16:35:39.565+0200",
  "_id": "X1VcWngBQzhG6Dcr9eN_"
}
```

Figure 15: Security alert details in JSON format



Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
2021-03-22 16:39:33			Guardian AST alert - CONNECTION_LOST - Guardian AST connection lost with 160.40.53.200	9	100023
2021-03-22 16:39:27			Guardian AST alert - Command execution from 160.40.53.200 - In-Tank Status Report.	10	100027
2021-03-22 16:39:23			Guardian AST alert - Command execution from 160.40.53.200 - Shift Report.	10	100029
2021-03-22 16:35:39			Guardian AST alert - Command execution from 160.40.53.200 - In-Tank Leak Detect Report.	10	100026
2021-03-22 16:35:35			Guardian AST alert - Command execution from 160.40.53.200 - Delivery Report.	10	100028

Figure 16: Detected security incidents (connection lost, I20400, I20500)

Description of the Tool Demo

A demo use case can be designed in collaboration with the Penetration Testing tool which can act as the attacker in the deployed demo scenario. CTI Extractor will extract CTI data from an intentionally vulnerable machine such as the one described in section 3.1.1, using internal data collection functionalities along with machine learning threat detection. Subsequently the extracted CTI is converted to STIX 2.1, validated according to the STIX 2.1 standard, and becomes available for sharing.

Apart from common services such as Joomla CMS, Apache and databases, the amount of available services will be extended with various Industrial Control Systems (ICS) services (e.g., Modbus, SCADA) which are equally likely to be targeted by the attacker. Upon the attack on the VM that is performed by the Penetration Testing tool, CTI Extractor will detect the threats in real-time. The identified threats will be correlated with previous CTI data in the by utilising the correlation functionality of CTI Extractor and the STIX bundles will be enriched with the newly detected data. Prior to sharing the enriched STIX bundle, the data is once more validated in order to ensure the integrity of the CTI data.

Tool related questions

Question #17.1.CTI_E

Did the extracted CTI help to better understand the security risks and vulnerabilities of the system?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Question #17.2.CTI_E

Was the tool able to detect threats in real time?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Question #17.3.CTI_E

Was the extracted CTI displayed to you in an intuitive and visually appealing way?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

If No, do you have any suggestions regarding the improvement of the user interface?

Expected category of answer: **[textbox]**

Question #17.4.CTI_E

Would you consider using CTI Extractor in your organisation?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

If the user replies No, a further question appears

If no, do you have any suggestions regarding the improvement of the tool?

Expected category of answer: **[textbox]**

Question #17.5.CTI_E

How would you describe your overall experience with the tool?

Expected category of answer: **[choice]**

Option list for answer: [Scale 1-10]

3.1.7 MonSys Bridge

Description of the Tool

The dynamic monitoring of services availability and cybersecurity situational awareness is critical for today's business, economic and critical infrastructures. Turning the somewhat fragmented or accident-driven cybersecurity efforts of both public and private organizations into data-driven and research-informed consistent efforts is paramount for the delivery of consistently superior and safer digital services. Furthermore, many organizations already use their own set of tools to monitor their systems. In most cases, however, the know-how and intelligence gained through the use of such utilities will remain within the organization.

Through the MonSys Bridge, ECHO provides an easy way to incorporate the functionalities and information of external monitoring solutions within the ECHO Early Warning System. Thus, the MonSys Bridge allows public and private organizations, regardless of their size or industry sector, to benefit from the ECHO Early Warning System while still using their preferred monitoring solution, and thus contribute with anonymized cybersecurity intelligence to the European cybersecurity situational awareness and knowledge-sharing.

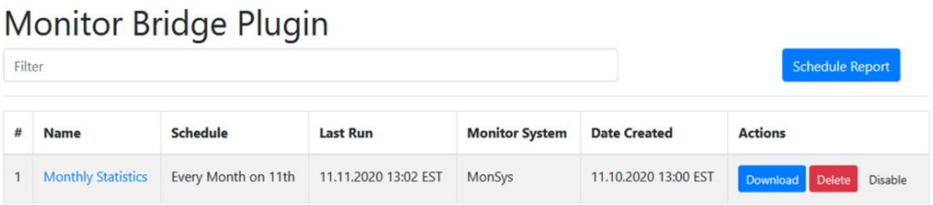
The MonSys Bridge is a universal data exchange plugin, through which external monitoring systems could be integrated with the following functionalities within the ECHO Early Warning System:

1. Based on predefined criteria, alerts in external monitoring solutions automatically generate a ticket and/or warnings in the E-EWS through the MonSys Bridge.
2. The MonSys Bridge automatically generates, uploads, and updates report from external monitoring systems to the E-EWS based on a predefined schedule, template, and criteria.
3. The MonSys BridgeChoose an item. automatically uploads and dynamically updates visualizations (graphs, charts, maps, etc.) from the external monitoring system to the E-EWS.

Thus, the MonSys Bridge supplements the functionalities of the monitoring solutions of its users, with the functionalities of the E-EWS, being tested with three external monitoring tools, namely MonSys, Zabbix, and Grafana.

The long-term goal of the research and development team is to explore automation and noise reduction/ priority modification of the incoming alerts through the implementation of a machine learning layer.

The MonSys Bridge has a simple, easy-to-use, and intuitive GUI, to support the scheduling process and facilitate the review of reports.

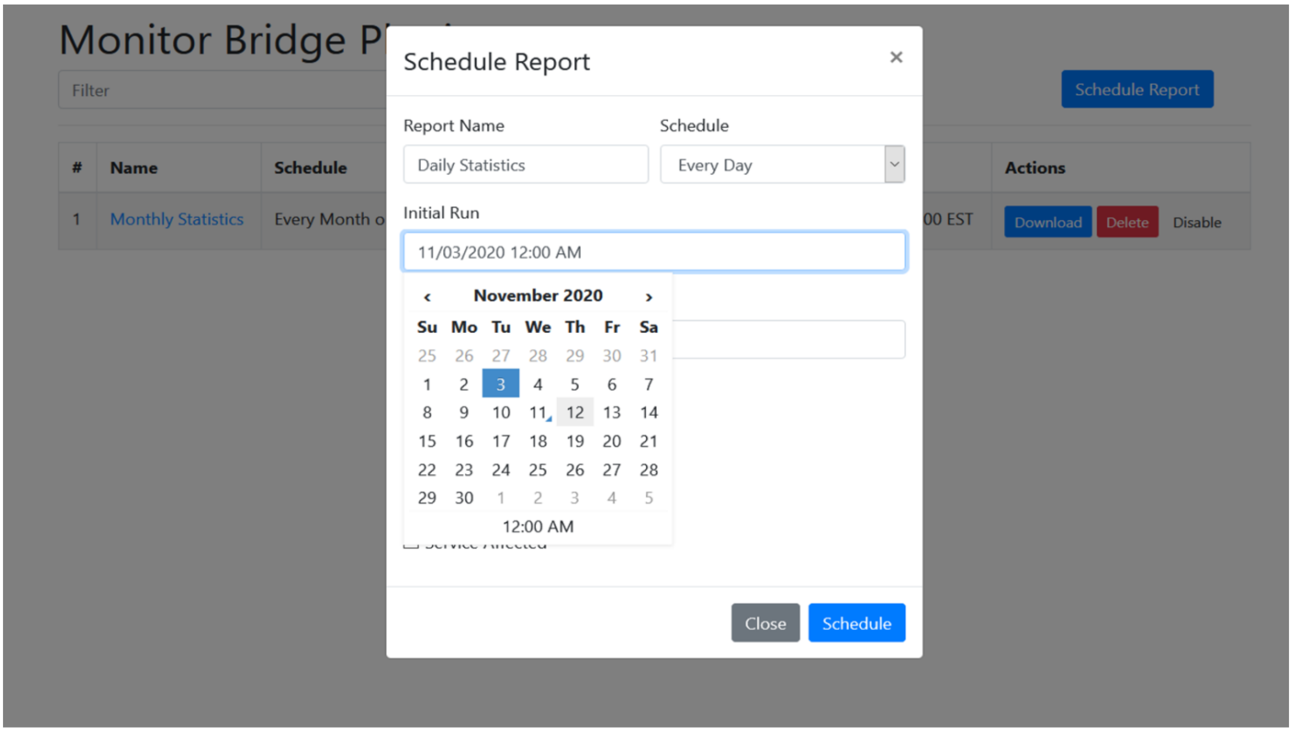


Monitor Bridge Plugin

#	Name	Schedule	Last Run	Monitor System	Date Created	Actions
1	Monthly Statistics	Every Month on 11th	11.11.2020 13:02 EST	MonSys	11.10.2020 13:00 EST	Download Delete Disable

Figure 17: MonSys Bridge: GUI Screenshot 1, General Interface

Should a user need to schedule another report, this can be achieved through the schedule report interface, as shown below in Figure 18.



Monitor Bridge P
Filter
Schedule Report
# Name Schedule Actions
1 Monthly Statistics Every Month o 00 EST Download Delete Disable

Schedule Report

Report Name: Daily Statistics

Schedule: Every Day

Initial Run: 11/03/2020 12:00 AM

November 2020

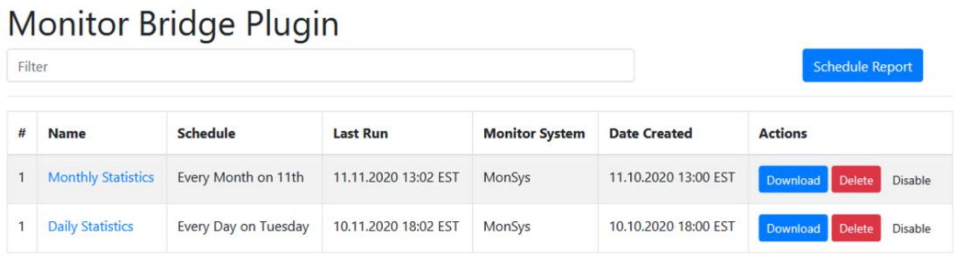
Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

12:00 AM

Figure 18: MonSys Bridge: GUI Screenshot 2, Scheduling a Report

Scheduling a report is made easy through the interface, providing calendar functionality and a scheduler. Both of these functionalities have built-in validation, allowing users to schedule only reports in a reasonable timeframe, as defined by the system functionalities.

Below we see that the report has already been generated:


Monitor Bridge Plugin

#	Name	Schedule	Last Run	Monitor System	Date Created	Actions
1	Monthly Statistics	Every Month on 11th	11.11.2020 13:02 EST	MonSys	11.10.2020 13:00 EST	Download Delete Disable
1	Daily Statistics	Every Day on Tuesday	10.11.2020 18:02 EST	MonSys	10.10.2020 18:00 EST	Download Delete Disable

Figure 19: MonSys Bridge: GUI Screenshot 3, Daily Statistics Report Generated

Description of the Tool Demo

he general level of security of the actors in the European Digital Single Market depends not only on their effort but also on the coordinated actions of the entire socio-economic environment. Due to the complex and heterogeneous nature of the cybersecurity landscape and the ever-evolving cyber threats, the ecosystem needs to ensure, even at the micro-organizational level, adequate cybersecurity situational awareness at least of the supply chain of the organization. The effective exchange of information could reduce significantly the destructive impact and cascading effects of cyber attacks.

One of the main challenges in this process is preserving the intellectual property rights, fundamental data privacy rights, and reputation of the businesses. The MonSys Bridge contributes to the establishment of a trust model of information sharing through the anonymization and secure exchange of data based on predefined criteria, fully under the users' control. Meanwhile, the MonSys Bridge provides additional benefits to the users by delivering them key information about affected ICT systems, vulnerabilities, threats, and attacks of interest to them through the E-EWS.

Last but not least, the MonSys Bridge enhances the cybersecurity intelligence capabilities of the EU market actors and responsible public authorities enriching the library of the E-EWS with data collected by organizations that might not join the E-EWS or might not be willing to share incident-related information in other circumstances.

Tool related questions

Question #17.1.MonSys

Does your organization already use a web or network availability monitoring system or an intrusion detection system?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Il the user replies “Yes”, a new question appears

If yes, could you, please, specify?

Expected category of answer: **[textbox]**

Question #17.2.MonSys

What type of anonymized information would be willing to exchange with stakeholders, both within your supply chain and external?

Expected category of answer: **[choice]**

Option list for answer: [Exact Incident Time
Number of Affected Applications
Affected Applications
Severity Status
Fingerprint
Incident Type (such as HTTPS down, etc.)
Server OS Version]

3.1.8 Malware Analysis and Intelligence Tool

Description of the Tool

The proposed tool is an automated and behaviour-based malware analysis toolkit that is going to identify potential malicious executables files (.exe, .dll) and collect Cyber Threat Intelligence for the file by using online resources.

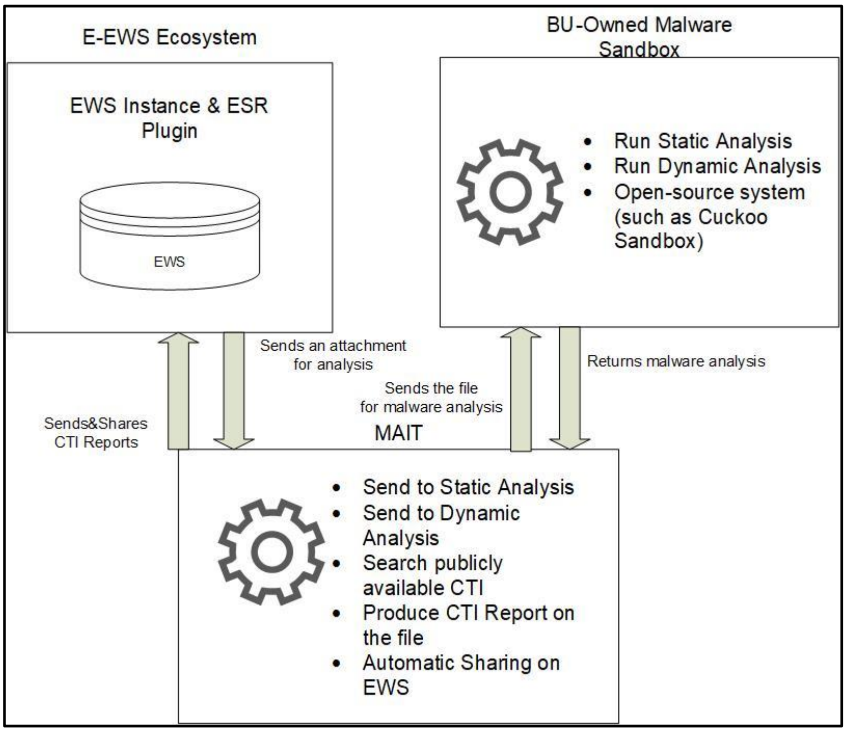


Figure 20: Malware Analysis and Intelligence Tool – Structural architecture

The contents of the report include (but are not limited to) the following:

- Chronological data about the malicious file, i.e. first appearance, increase in time.
- Any weaponisation in any APT campaigns or cyberattacks in general.
- Public information on cyber attribution.
- Related vulnerabilities and information on the relevance.

The tool will seamlessly integrate with the E-EWS system to share this information as a cyberticket within the organisation and with member constituencies/organisations.

Malware Analysis

Given the malicious file, malware analysis is conducted on both static and dynamic level. The details for both analyses are as follows:

The static analysis will provide useful metadata and information which can be used as input in the final malware analysis report. The reported information will include: • Entropy calculation of the executable file. • MD5, SHA1, SHA256 hash calculation of the malware. • Extraction of textual features of the executable file. • The impfuzzy library, calculate hashes from the import API of PE files.	**The dynamic analysis** will provide useful metadata and information on malware execution and behaviour. The information collected can be used as input in the final malware analysis report. The reported information will include: • Cuckoo sandbox analysis results. • Network monitoring and C&C communication results. • Disk and function-call usage monitoring results. • DLL library injects information.

• Extraction of metadata from Microsoft Office documents, pdf files using the libraries pdfinfo, officemeta.	• Memory injection analysis and inspection results. • Packing/obfuscation/encryption information • Downloaded external malicious files

Collecting Cyber Threat Intelligence (CTI)

Applying malware intelligence and identifying the aforementioned interrelationships can aid in establishing shared behaviour, authorship, and provenance, evolutionary artefacts and lineage, author profiles, follow the trends in malware and possibly designate relationships between attack groups; leading to cyber attribution and deterrence. Based on extracted data (resulting from static and dynamic analysis) and identified attack vectors (resulting from dynamic analysis) the following malware intelligence can be collected and reported:

- Results from scanning the sample in online sources, VirusTotal, AlienVault, MalwareBazaar, URLHaus, SecurityTrails, Threat Intelligence Platform, IP2Proxy.
- MITRE | ATT&CK methodologies, mapped to malware functionality.
- Chronological data about the malicious file, i.e. first appearance, increase in time.
- Publicly available weaponisation in any APT campaigns.
- Publicly available information on cyber attribution.
- Related vulnerabilities and information on relevance.
- Digital Signatures of the malicious executable

Description of the Tool Demo

Demonstration of this tool includes extracting the artefacts from static and dynamic analyses presenting the analysis results in json format within the developed UI. Moreover, demonstration will show collection of CTI for the provided samples, mapping the results to ATT&CK navigator.

The tool contains an extended analysis sections for URL and IP intelligence collection; these are included in the demonstration provided with the malicious URL and IP samples.

Tool related questions

Question #17.1.MAIT

Did the MAIT tool helped you identify and make use of valuable metadata information, related to the malicious executable under investigation, as given by the static and the dynamic analysis functionalities?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Il the user replies “No”, a new question appears

If No, please briefly describe what kind of information could be added in these functionalities or comment on any way towards their improvement

Expected category of answer: **[textbox]**

Question #17.2.MAIT

Were you able to extract and apply to your work valuable CTI information, given by the respective functionality of the MAIT tool?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Il the user replies “No”, a new question appears

If No, please briefly describe what kind of CTI information could be added in this functionality or comment on any way towards its improvement

Expected category of answer: **[textbox]**

Question #17.3.MAIT

Did the MAIT tool help you identify interconnections or any kind of relation between the analysed malicious file and known APT campaigns?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Il the user replies “No”, a new question appears

If No, please briefly describe what kind of cyber attribution-related information could be added in this functionality or comment on any way towards its improvement

Expected category of answer: **[textbox]**

Question #17.4.MAIT

Did you find the automatic identification and mapping of the related TTPs to the ATT&CK Navigator useful?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Il the user replies “No”, a new question appears

If No, please briefly describe in which way did this approach negatively affect you, and your work

Expected category of answer: **[textbox]**

Question #17.5.MAIT

Was the front-end part of MAIT tool user-friendly; did it present the given information in a well-structured way?

Expected category of answer: **[choice]**

Option list for answer: [Yes, No]

Il the user replies “No”, a new question appears

If No, please briefly describe in which way you had difficulties in using the tool or making use of the provided information

Expected category of answer: **[textbox]**

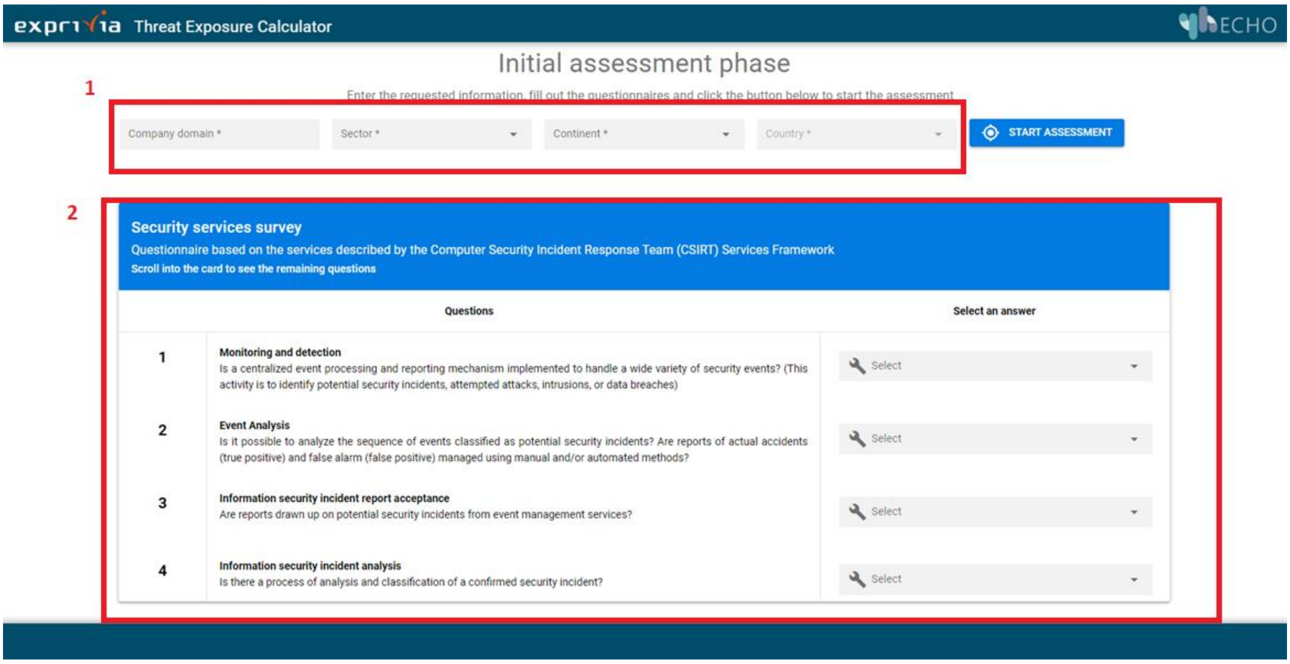
3.1.9 Threat Exposure Calculator

Description of the Tool

The **Threat Exposure Calculator** aims to calculate the current level of exposure concerning the main threats and subsequently to promptly provide targeted solutions tailored to the customer. The evaluation of the actual security situation is obtained starting from a passive analysis of the customer and an active interaction with the IT specialists.

The passive analysis is performed using tools designed to identify vulnerabilities regarding web portals owned by the customer. This analysis is carried out exclusively from the external perimeter of the corporate network and is capable of monitoring vulnerabilities visible from the outside. In Figure 21, is boxed in red and numbered as 1 the part of the interface where the user can easily specify the perimeter:

- domain url of the company;
- sector of interest of the company: cloud, critical infrastructure, entertainment, finance, healthcare, multiple, public administration, research-education, retail;
- continent: multinational, America, Asia, Europe, Africa, Oceania;
- country: depends on the previous selection (note that not all the countries are actually covered).



Initial assessment phase

Enter the requested information, fill out the questionnaires and click the button below to start the assessment

Security services survey

Questionnaire based on the services described by the Computer Security Incident Response Team (CSIRT) Services Framework

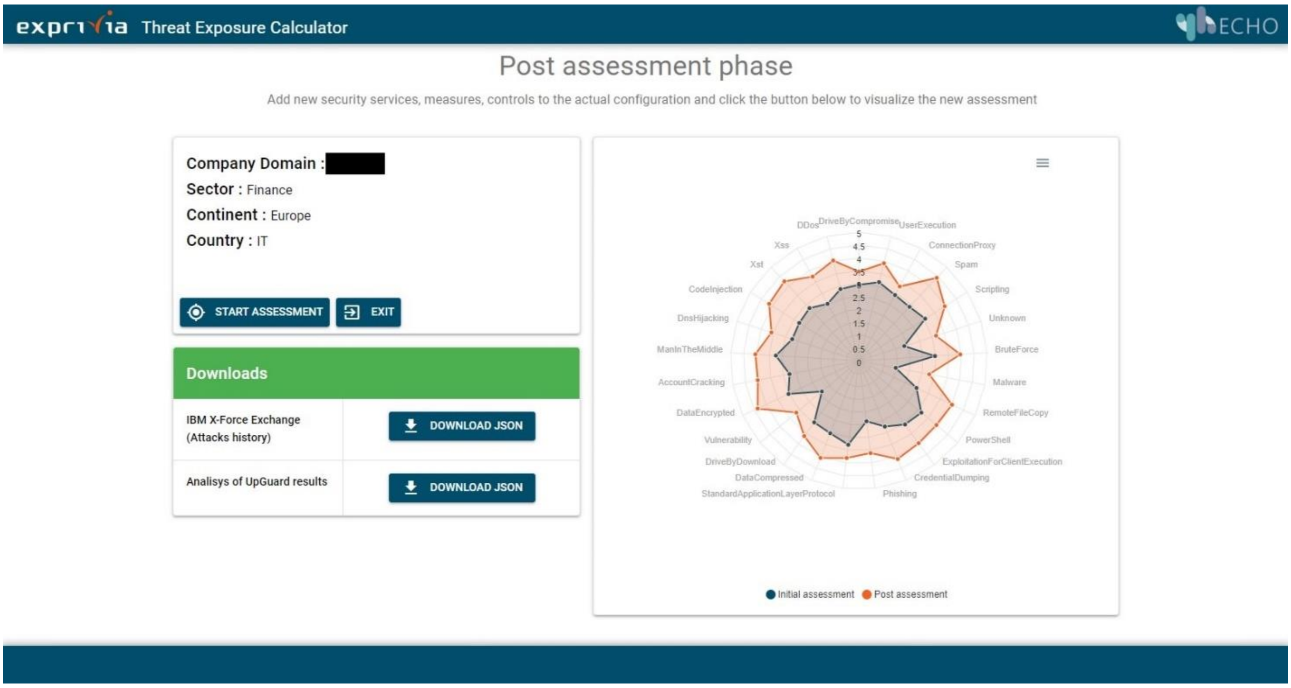
Scroll into the card to see the remaining questions

	Questions	Select an answer
1	**Monitoring and detection** Is a centralized event processing and reporting mechanism implemented to handle a wide variety of security events? (This activity is to identify potential security incidents, attempted attacks, intrusions, or data breaches)	Select
2	**Event Analysis** Is it possible to analyze the sequence of events classified as potential security incidents? Are reports of actual accidents (true positive) and false alarm (false positive) managed using manual and/or automated methods?	Select
3	**Information security incident report acceptance** Are reports drawn up on potential security incidents from event management services?	Select
4	**Information security incident analysis** Is there a process of analysis and classification of a confirmed security incident?	Select

Figure 21: TEC - First Costumer Survey

The active analysis requires the intervention of IT specialists to investigate the security mechanisms (services and measures) implemented in the internal perimeter. This phase is intended to discover what the customer uses to create a defence-and-response mechanism against cyber threats. In Figure 21, is boxed in red and numbered as 2 the questionnaire phase, there is no information that the customer has necessarily to provide but, at the same time, for a more accurate analysis, it would be useful to know better the implemented security mechanisms. Customer questions will range from CSIRT-compliant security services to vulnerability management.

After this data has been collected, the plugin reports the actual level of exposure to threats viewable in a radar chart, based on the main threats in that business sector and proposes solutions in terms of technology and security measures that must be adapted to change the security level of the company. The actual level of exposure to threats is calculated based on information related to the company location and the work sector. In Figure 22, is reported as a radar chart the output of the assessment and what is obtained after an evaluation of the impact of hypothetic measures and control implemented.



Post assessment phase

Add new security services, measures, controls to the actual configuration and click the button below to visualize the new assessment

Company Domain : [redacted]
Sector : Finance
Continent : Europe
Country : IT

Downloads

IBM X-Force Exchange (Attacks history)	DOWNLOAD JSON
Analisys of UpGuard results	DOWNLOAD JSON

Figure 22: TEC - Comparison Assessment chart

The prototype is designed to be easily integrated with other external tools indeed there is a mapping between the elements used by the assessment engine and the output of the external tools.

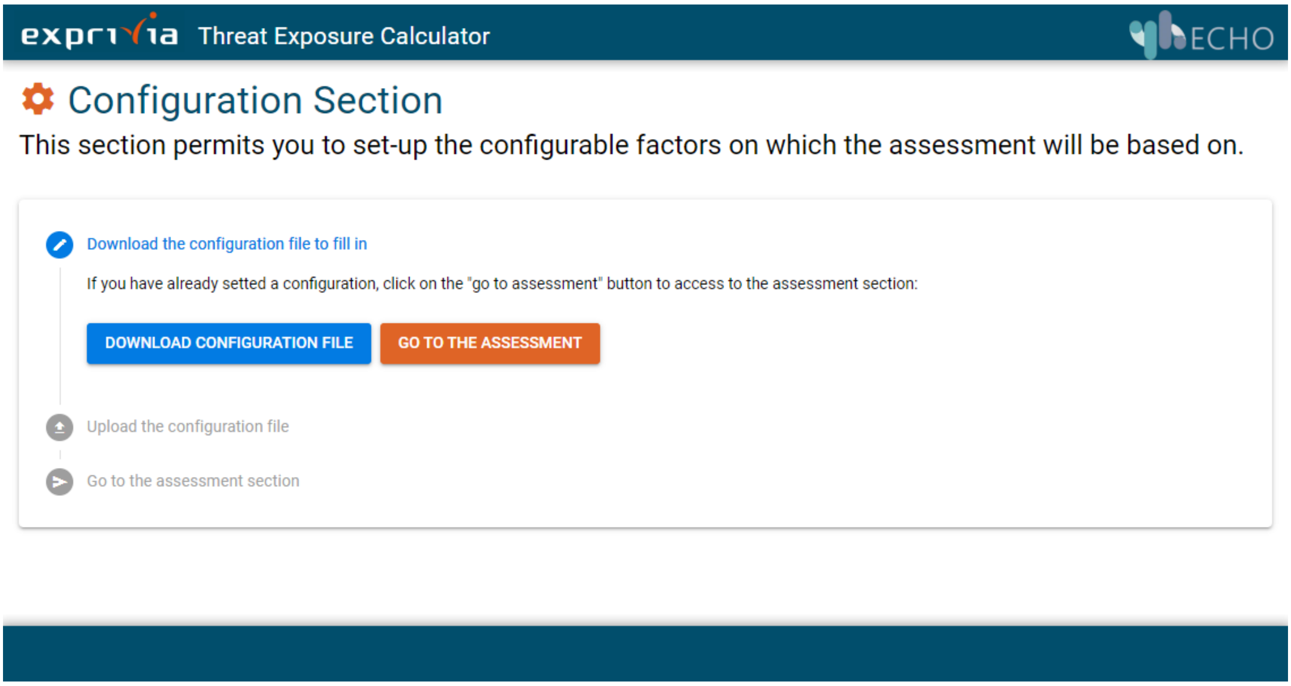
Description of the Tool Demo

This subsection contains several graphical user interface screenshots depicting the main functionality of the Threat Exposure Calculator (TEC) web application with the supportive description.

The steps to follow to generate the initial and post-assessment are as follows:

1. Download the configuration file.
2. Make changes to the configuration file and upload it.
3. Fill in the form with the customer's data.
4. Fill in with the customer the two surveys relating to the security controls implemented by the company.
5. Click on the Start Assessment button and wait for the assessment to be done.
6. Configure the security controls that will be adopted and perform post-assessment.

Figure below depicts step 1.



exprivia Threat Exposure Calculator
ECHO

Configuration Section

This section permits you to set-up the configurable factors on which the assessment will be based on.

Download the configuration file to fill in

If you have already setted a configuration, click on the "go to assessment" button to access to the assessment section:

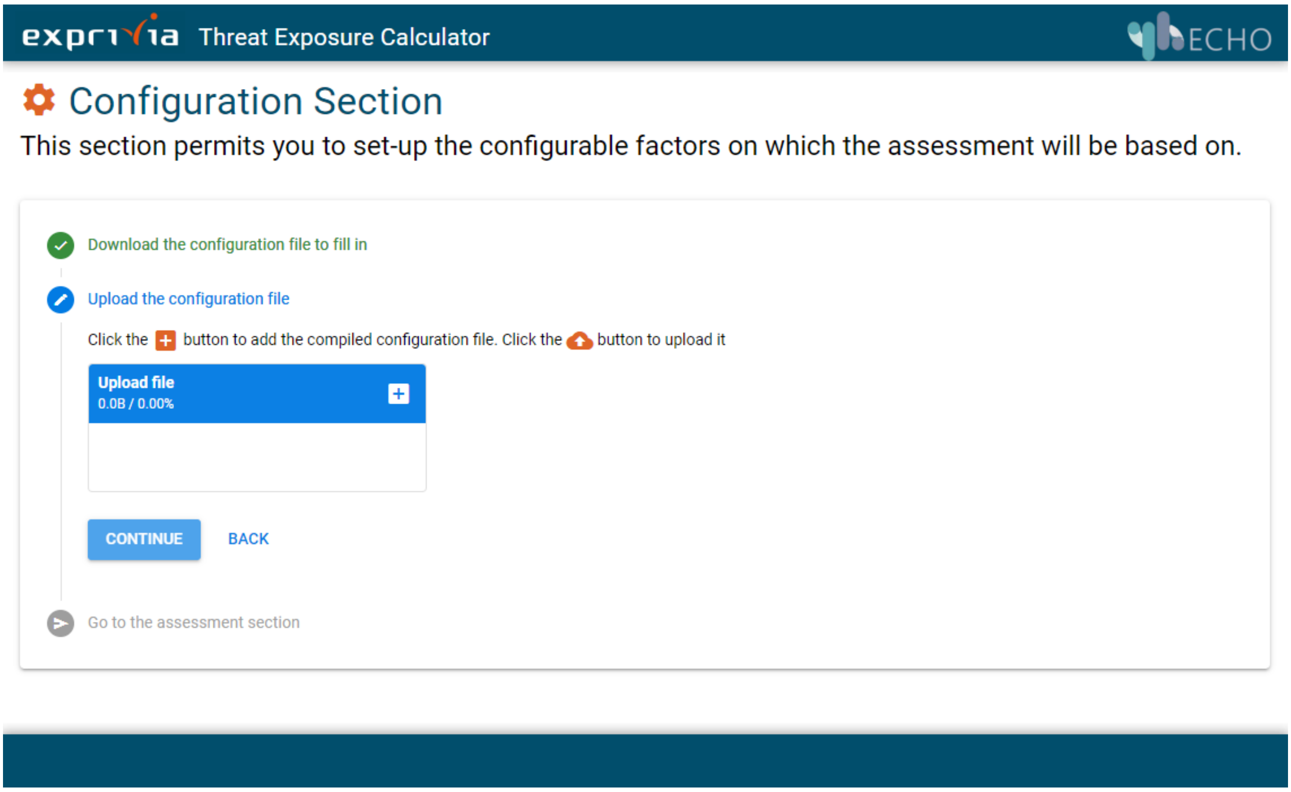
DOWNLOAD CONFIGURATION FILE
GO TO THE ASSESSMENT

Upload the configuration file

Go to the assessment section

Figure 23: TEC – Configuration Section, download

It is possible to download a default configuration .json file (Figure 23) and make any necessary changes. Various parameters can be configured, including states and continents with the relative risk indices. Moreover, one needs to indicate available licenses of Nessus, Upguard, IBM Exchange X-Force. After compiling the configuration file, it must be uploaded (Figure 24).



Configuration Section

This section permits you to set-up the configurable factors on which the assessment will be based on.

✓ Download the configuration file to fill in

Upload the configuration file

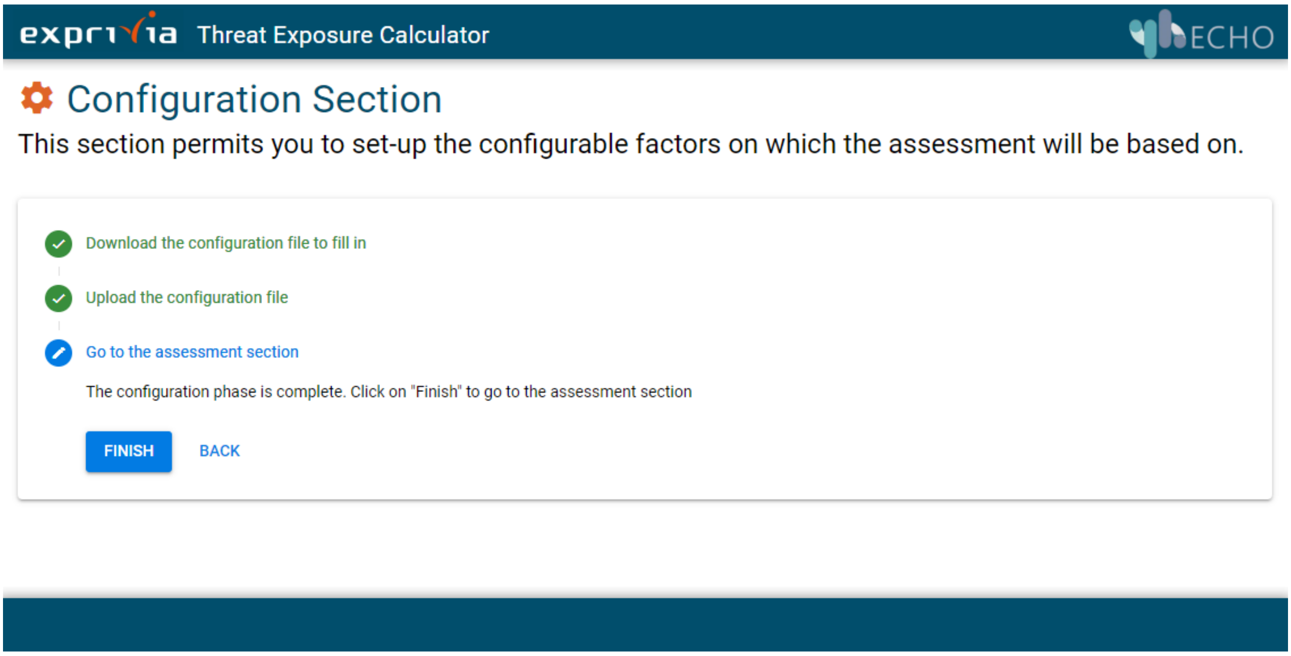
Click the + button to add the compiled configuration file. Click the button to upload it

Upload file
0.0B / 0.00%

Go to the assessment section

Figure 24: TEC – Configuration Section, upload

After uploading the file, clicking on the "Finish" button (Figure 25) will move forward to the assessment section (see Figure 26).



Configuration Section

This section permits you to set-up the configurable factors on which the assessment will be based on.

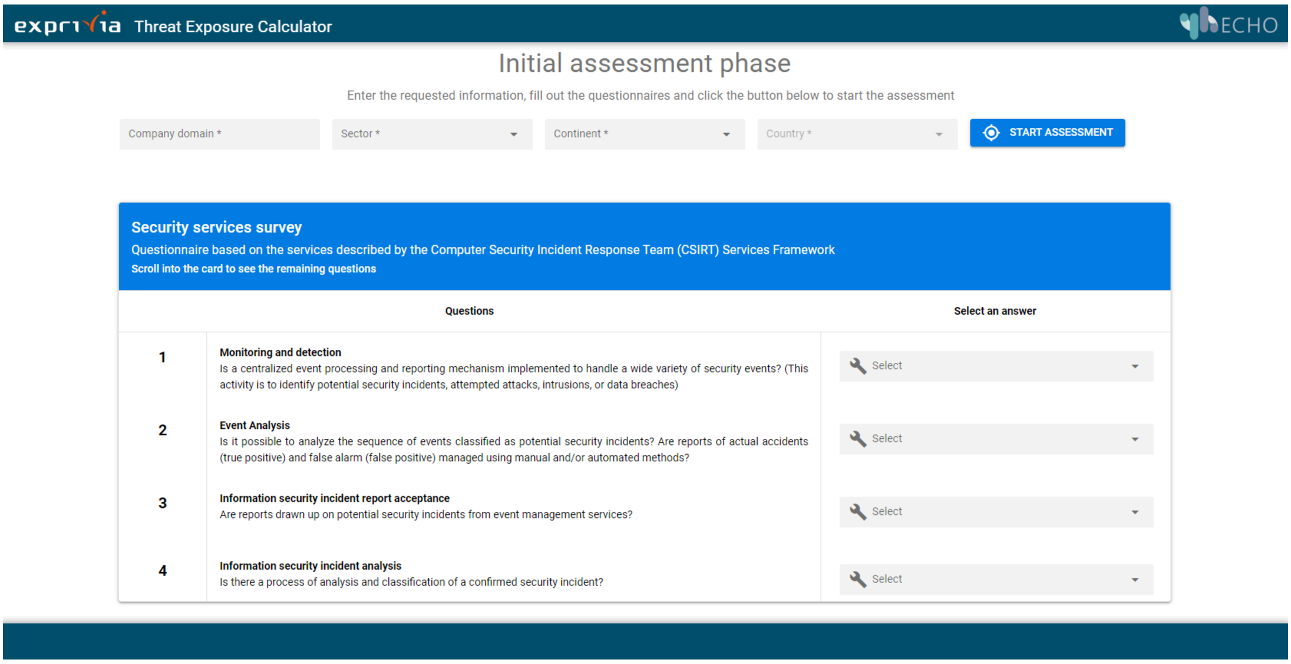
✓ Download the configuration file to fill in

✓ Upload the configuration file

Go to the assessment section

The configuration phase is complete. Click on "Finish" to go to the assessment section

Figure 25: TEC – Configuration Section, finish configuration



Initial assessment phase

Enter the requested information, fill out the questionnaires and click the button below to start the assessment

Security services survey

Questionnaire based on the services described by the Computer Security Incident Response Team (CSIRT) Services Framework

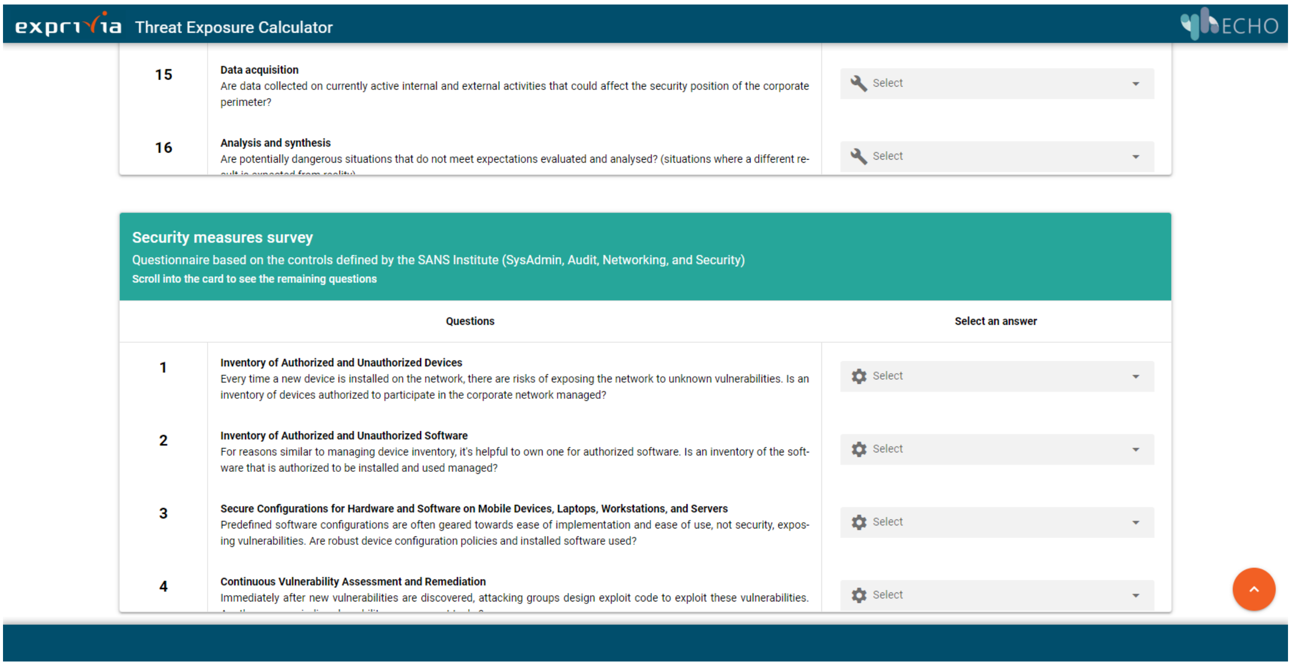
Scroll into the card to see the remaining questions

	Questions	Select an answer
1	**Monitoring and detection** Is a centralized event processing and reporting mechanism implemented to handle a wide variety of security events? (This activity is to identify potential security incidents, attempted attacks, intrusions, or data breaches)	Select
2	**Event Analysis** Is it possible to analyze the sequence of events classified as potential security incidents? Are reports of actual accidents (true positive) and false alarm (false positive) managed using manual and/or automated methods?	Select
3	**Information security incident report acceptance** Are reports drawn up on potential security incidents from event management services?	Select
4	**Information security incident analysis** Is there a process of analysis and classification of a confirmed security incident?	Select

Figure 26: TEC - First Costumer Survey

In addition to the configuration file, the input data to the tool (provided in Figure 27) are:

- Company URL (e.g., “exprivia.it”).
- Sector in which the company operates (e.g. Healthcare, Critical Infrastructure, Finance, etc.).
- Continent, where the company has physical headquarter.
- Country, where the company has physical headquarter.
- Customer responses to questionnaire based on the services described by the Computer Security Incident Response Team (CSIRT) Services Framework (Figure 26).
- Customer responses to questionnaire based on the controls defined by the SANS (SysAdmin, Audit, Networking, and Security) Institute.



15	**Data acquisition** Are data collected on currently active internal and external activities that could affect the security position of the corporate perimeter?	Select
16	**Analysis and synthesis** Are potentially dangerous situations that do not meet expectations evaluated and analysed? (situations where a different result is expected from reality)	Select

Security measures survey

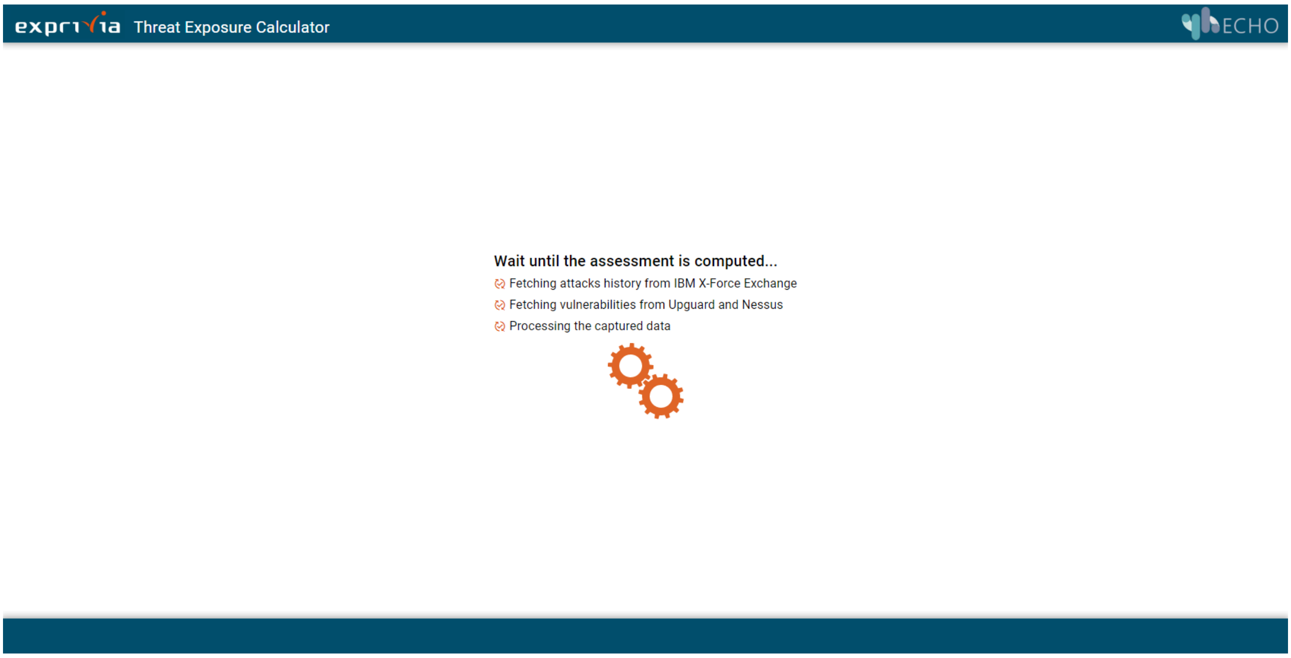
Questionnaire based on the controls defined by the SANS Institute (SysAdmin, Audit, Networking, and Security)

Scroll into the card to see the remaining questions

	Questions	Select an answer
1	**Inventory of Authorized and Unauthorized Devices** Every time a new device is installed on the network, there are risks of exposing the network to unknown vulnerabilities. Is an inventory of devices authorized to participate in the corporate network managed?	Select
2	**Inventory of Authorized and Unauthorized Software** For reasons similar to managing device inventory, it's helpful to own one for authorized software. Is an inventory of the software that is authorized to be installed and used managed?	Select
3	**Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers** Predefined software configurations are often geared towards ease of implementation and ease of use, not security, exposing vulnerabilities. Are robust device configuration policies and installed software used?	Select
4	**Continuous Vulnerability Assessment and Remediation** Immediately after new vulnerabilities are discovered, attacking groups design exploit code to exploit these vulnerabilities.	Select

Figure 27: TEC – Second Costumer Survey

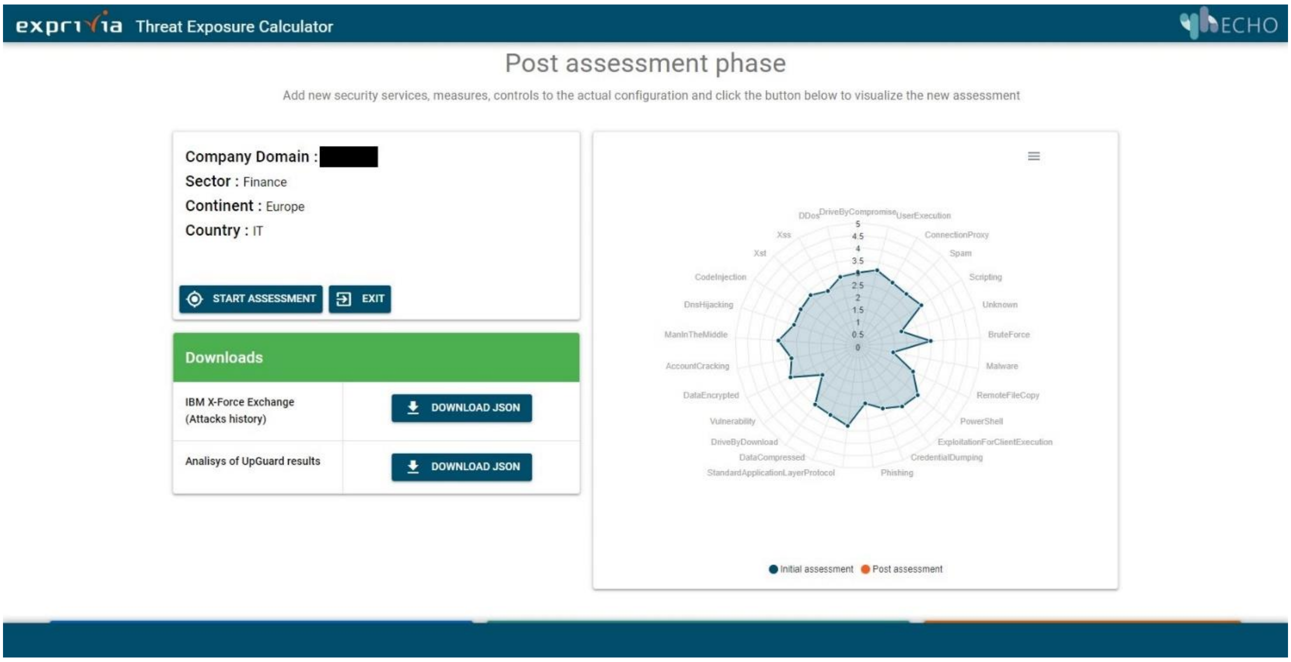
The assessment begins by clicking on the “Start Assessment” button. Information is retrieved from external data sources (e.g. UpGuard, IBM Exchange X-force, Exprivia Threat Intelligence Report, etc.) and at the end of the computation, the radar chart relating to the initial assessment is generated (Figure 28 and Figure 29).



Wait until the assessment is computed...

- Fetching attacks history from IBM X-Force Exchange
- Fetching vulnerabilities from Upguard and Nessus
- Processing the captured data

Figure 28: TEC – Assessment in progress



Post assessment phase

Add new security services, measures, controls to the actual configuration and click the button below to visualize the new assessment

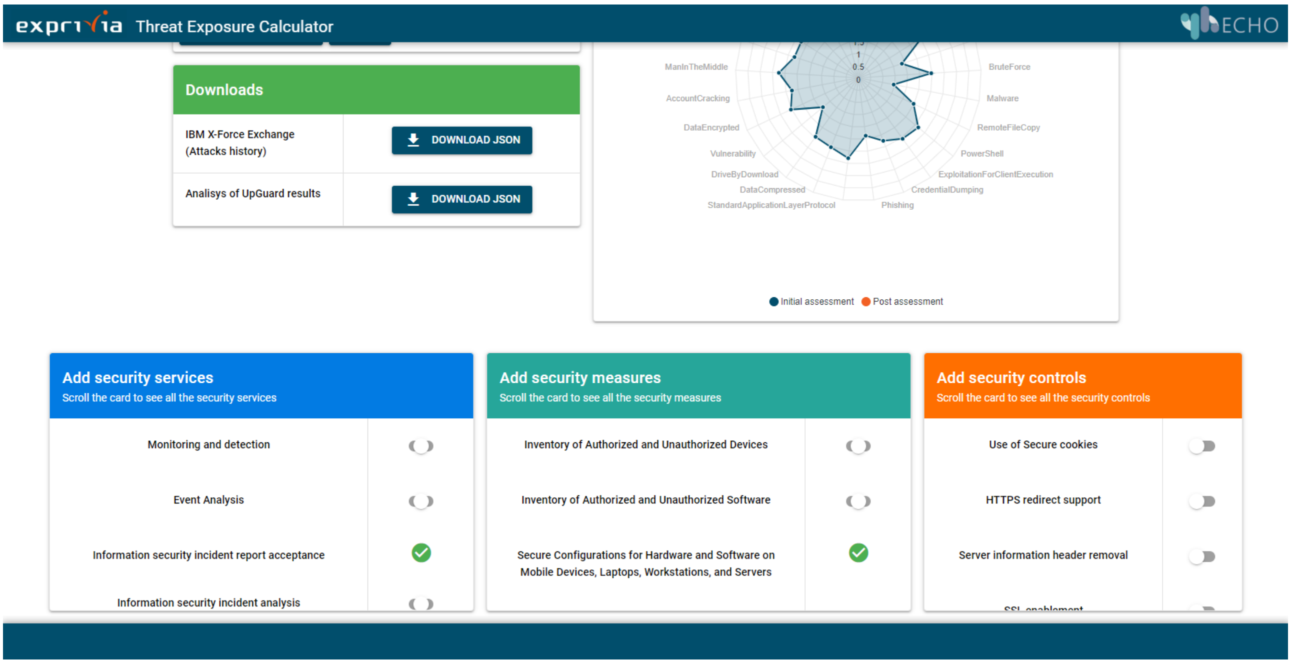
Company Domain : [redacted]
Sector : Finance
Continent : Europe
Country : IT

Downloads

IBM X-Force Exchange (Attacks history)	DOWNLOAD JSON
Analisys of UpGuard results	DOWNLOAD JSON

Figure 29: TEC - Initial Assessment chart

At the end of the computation, it is also possible to download the reports provided by the external data sources and download the radar chart in png, svg and csv format (Figure 29).



Downloads

IBM X-Force Exchange (Attacks history)	DOWNLOAD JSON
Analisys of UpGuard results	DOWNLOAD JSON

Add security services
Scroll the card to see all the security services

Monitoring and detection	○
Event Analysis	○
Information security incident report acceptance	✓
Information security incident analysis	○

Add security measures
Scroll the card to see all the security measures

Inventory of Authorized and Unauthorized Devices	○
Inventory of Authorized and Unauthorized Software	○
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	✓

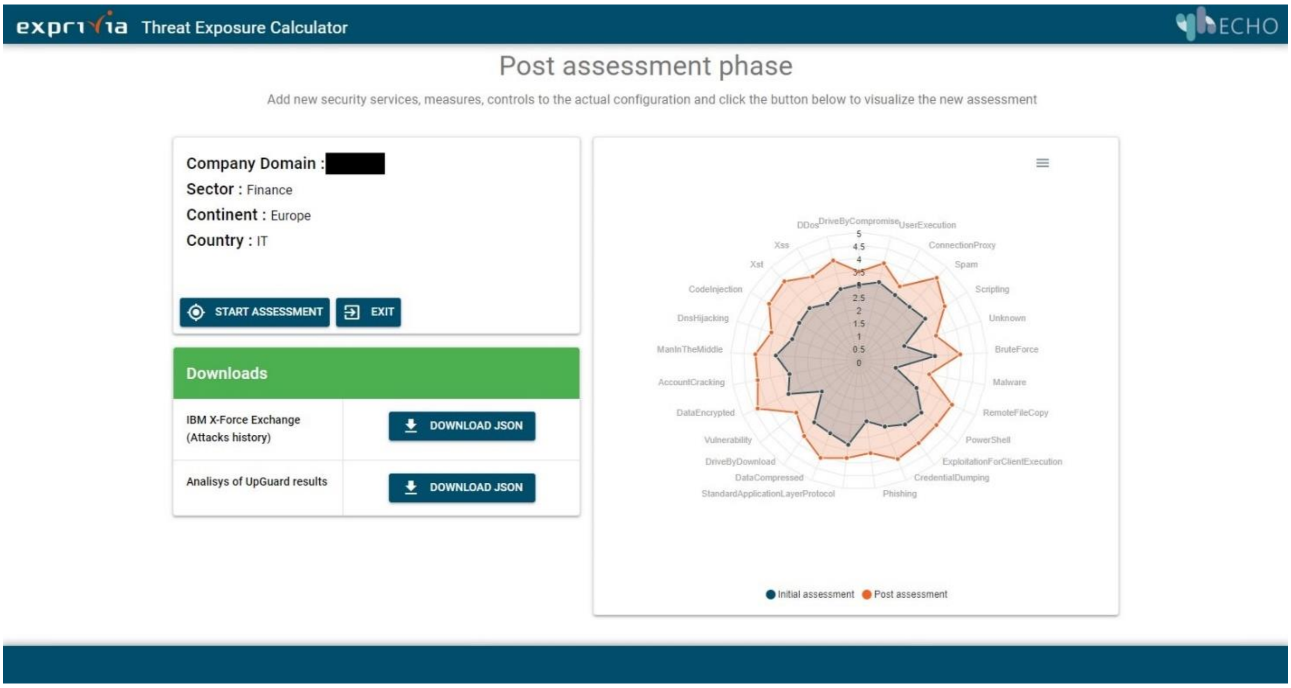
Add security controls
Scroll the card to see all the security controls

Use of Secure cookies	○
HTTPS redirect support	○
Server information header removal	○
SSL enablement	

Figure 30: TEC – Post Assessment configuration

At the end of the initial assessment, it is possible to configure all the security controls that are not currently implemented within the organization and to perform the Post Assessment to evaluate the benefit of adopting a certain security control not present in its infrastructure (Figure 30).

After performing post-assessment, the related radar chart is generated (Figure 31).



exprivia Threat Exposure Calculator

Post assessment phase

Add new security services, measures, controls to the actual configuration and click the button below to visualize the new assessment

Company Domain : [redacted]
Sector : Finance
Continent : Europe
Country : IT

Downloads

IBM X-Force Exchange (Attacks history)	DOWNLOAD JSON
Analisys of UpGuard results	DOWNLOAD JSON

Figure 31: TEC – Post Assessment chart

Tool related questions

Question #17.1.TEC

How would you describe your overall experience with the product?

Expected category of answer: **[choice]**

Option list for answer: [scale 1-5]

The question aims to let the user to specify a value between 0 and 5 to summaries how the tools is self-explicable and easy to use. It is also important to understand if the final outputs expressed as radar charts is enough descriptive of the situation.

Question #17.2.TEC

Can you suggest one or more features to develop or tools to be integrated in the prototype?

Expected category of answer: **[textbox]**

The question aims to allow the user to specify in a free text are what are his/her impression of the overall features implemented and eventually determine the lacks in terms of features developed or on tools to integrate as sources of information of the tool.

3.1.10 IDS Combo

Description of the Tool

Modern technologies allow collecting, storing, and processing huge amounts of historical and current data related to the functioning of networks. Several methods and tools have been developed to use heterogeneous multisource security-related data, or 'big data,' with the purpose to detect intrusions, identify and analyse other anomalous behaviour. Every method has advantages and disadvantages and performance may vary widely depending on the type of cyberattack (intrusion). Existing methods exhibit inherent limitations while processing a huge volume and variety of data with different granularity.

IDS Combo (Intrusion Detection [System] Combined Methods Toolbox) instantiates a comprehensive framework based on developments in the field of Artificial Intelligence (AI) and Big Data Analytics. Proven and emerging machine learning (ML) technologies and methods enable a coherent process of design and development of an efficient and optimized intrusion detection system. This process spans the whole chain of important design considerations – the 'representation' problem (design of the feature space), design, training and testing of relevant models, and the output space (where the outputs of different methods are combined). All this is performed in a big data environment, comprising historical and current data, correlating log data, traffic characteristics and other event features to analyse the attack process.

In the proposed tool, a two-stage anomaly-based network intrusion detection process is adopted. We apply traditional approaches to feature selection, meta-heuristic techniques, and the built-in in some ensemble methods—Random Forests, popular gradients boosting techniques—feature ranking to select relevant features for consequent analysis. Then, a binary classification is performed to distinguish intrusive traffic from a normal one, using several ML techniques. If an anomaly is detected, the data is fed to a range of multinomial classifiers to improve the accuracy and predict the type of attack. To design IDS with a higher detection rate and lower false-positive rates, various schemes for output combination are tested. Approaches to combine the outputs of diverse prediction schemes have been the focus of our portfolio of solutions.

Capabilities

The general capabilities of IDS Combo are presented in the following table.

Category	Functionality	Description	Note
Logs aggregation	**Collect, store, and process historical and incoming data related to the functioning of the network**	IDS Combo collects and aggregates data on server and application logs, network traffic and	

Category	Functionality	Description	Note
		events, user activities, threat intelligence, etc.	
Alerting	**Intrusion detection**	IDS Combo processes stored and incoming data applying a set of methods (learning algorithms). Then a meta-classifier processes its outputs to identify an anomaly (intrusion, malicious event, …)	
	Attack classification	When an anomaly is detected, the data is fed to a range of multinomial classifiers to improve the accuracy and predict the type of attack	

Table 9: Capabilities of the IDS Combo tool

High-Level Structure View

The core of IDS combo consists of components for (1) pre-processing the data from network monitoring, contextual information, alerts and other related data (2) feature selection, (3) several components realising the selected classification methods, and (4) combination of the outputs of the selected methods (Figure 32). These components are realized and tested over a static dataset, split into training and testing sub-set. Then, part of the dataset is used to emulate a real-time data stream and thus to estimate the usability of the approach in real-time.

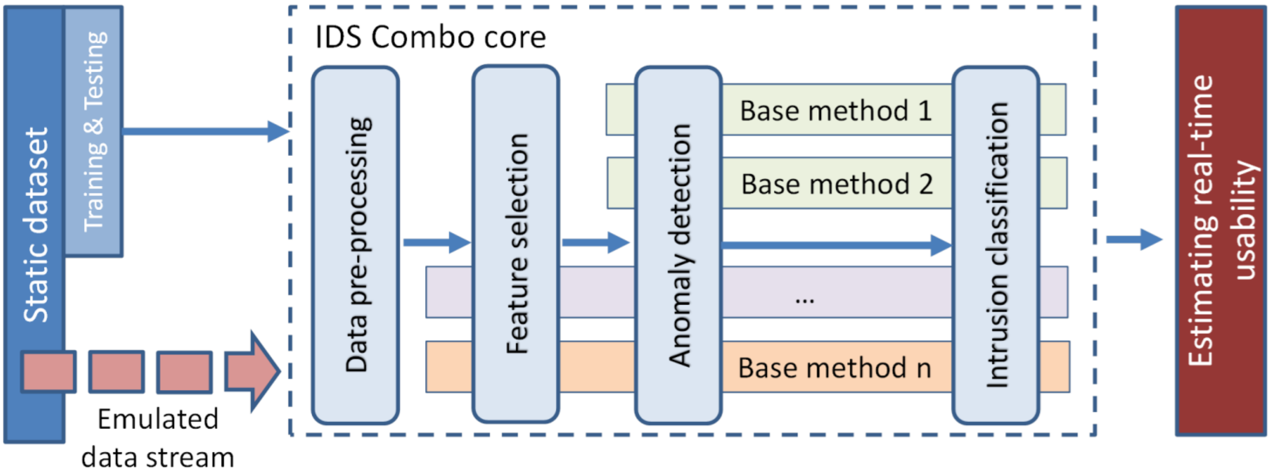


Figure 32: IDS Combo– Components and development workflow

Figure 33 visualizes the performance of selected classification methods in the achieved accuracy and F1-score over the NSL KDD dataset.

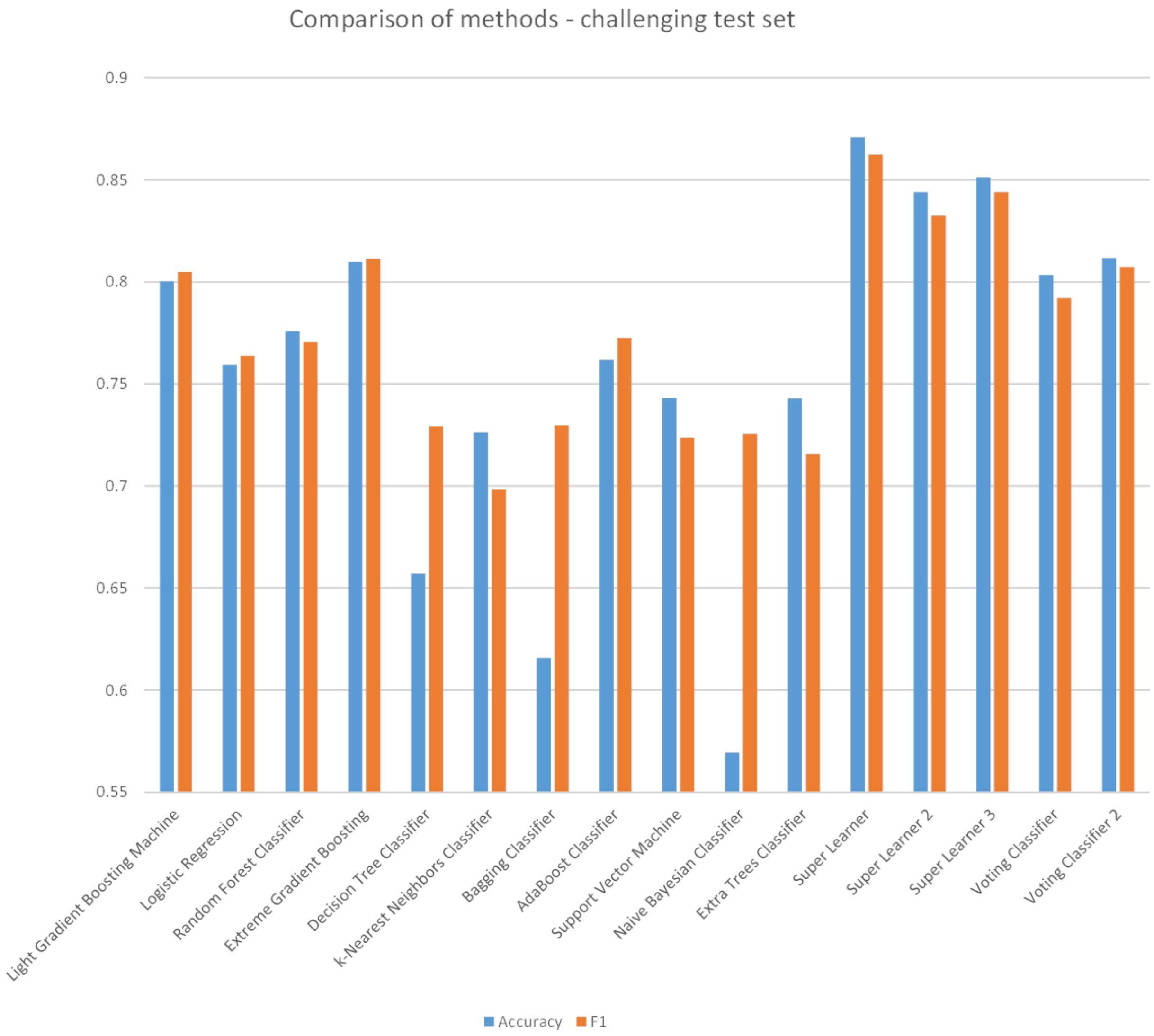


Figure 33: IDS Combo – Comparative performance of selected methods over the NSL KDD dataset

The actual implementation of IDS Combo is visualized in Figure 34. This envisions the realization of a set of sensors to capture the data from the monitored network and the service layer (including data storage and processing), interpretation of the outputs of IDS Combo, and visualization according to the needs of specific groups of users.

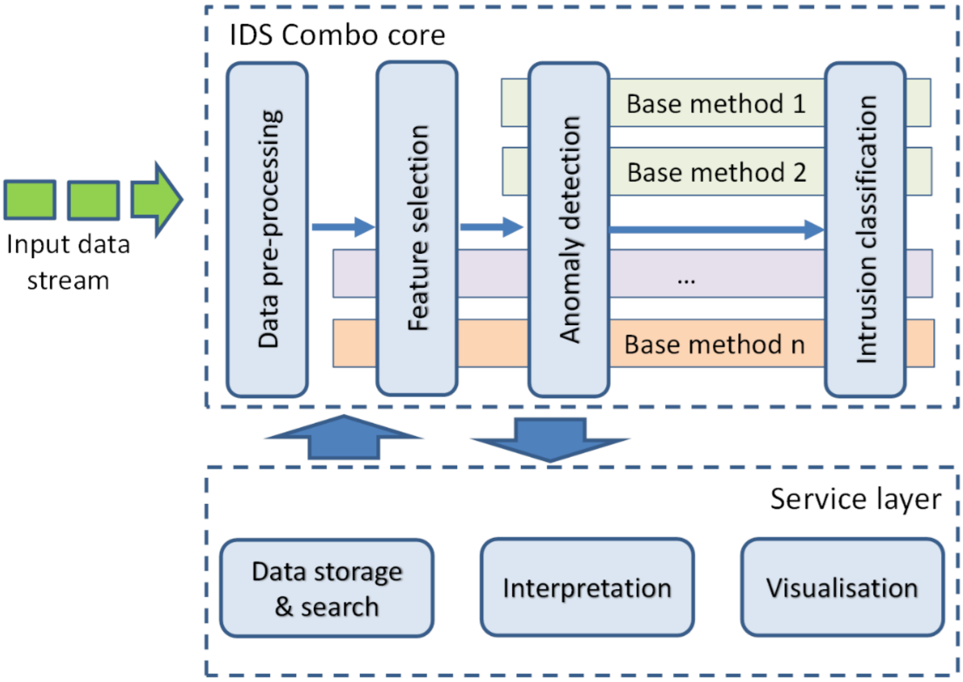


Figure 34: IDS Combo implementation mockup

Description of the Tool Demo

IDS Combo will be demonstrated in combination with MonSys Bridge (see section 3.1.7). Prior to the demonstrations, IDS Combo will be deployed in the network environment monitored by MonSys. In the preparation period IDS Combo will be adapted to this new environment in respect both to the data structure and to the specific threat landscape.

During the demonstration period, IDS Combo will be used to identify anomalies and classify intrusions (cyberattacks) over the incoming data stream.

Given that for a short period of time a real network is typically not subject of numerous attacks of different types and in order to provide for rigorous testing of IDS Combo, we will “enrich” the network data using recent datasets of cyberattacks, e.g., the most recent datasets provided by the Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick.[1]

[1] The last complete dataset, i.e., the one combining different types of attack, is CSE-CIC-IDS2018 from 2018. However, CIC has published a number of datasets per type of attack in 2019 and 2020.

Tool related questions

Question #17.1.IDS_C

How do you rate the usability of the tool? For the assessment of usability, please consider: does the tool seem to be effective, efficient, easy and intuitive.

Expected category of answer: **[choice]**

Option list for answer: [scale 1-10]

Question #17.2.IDS_C

To what extent IDS Combo provides for increased effectiveness of detection in terms of:

- ***Accuracy***
- ***Detection rate***
- ***False alert rate***
- ***F1-score***

Expected category of answer: **[textbox]**

Question #17.3.IDS_C

Is IDS Combo able to detect types of intrusions not seen during training (the preparation of the demo)?

- **How many unseen types of attack it was able to detect during the demo?**
- **How many unseen types of attack it was not able to detect during the demo?**

Expected category of answer: **[textbox]**

Question #17.4.IDS_C

Is the tool easy and intuitive to use?

Expected category of answer: **[choice]**

Option list for answer: [scale 1-10]

Question #17.5.IDS_C

How do you rate the completeness of the tool? For the assessment of the completeness, please consider: does the tool seem to be ready to use, not lacking important functionalities?

Expected category of answer: **[choice]**

Option list for answer: [scale 1-10]

Inter-sector prototypes should simplify the daily tasks of cybersecurity analysts and other professionals. The demo should clearly explain how to use the tool. Gathered feedback will let us know whether respondent perceived its usability as high or low.

3.1.11 E-MAT E-MAF Tool

Description of the Tool

As ECHO Multi-sector Assessment Framework (E-MAF, see [D2.2]) captures multiple inputs with the goal to analyse transversal and inter-sectoral challenges and opportunities in the aim of a complex framework. A software tool (E-MAT, web-based) can be created to lower the entry barrier of adoption and ease the usage to automate or guide application. It can be used as a demonstrator for E-MAF use cases and when designed accordingly can provide E-MAF assessment even without sharing the framework itself. It will increase the speed of developing E-MAF itself by creating the ability to analyse use-cases automatically. Its primary function will be to support Risk Management decision-making and to increase adoption.

A typical workflow of the E-MAT should look as depicted in Figure 35. In this picture it is clarified the main difference between E-MAF, an asset-free framework for Risk Assessment and Management by design, and its software tool implementation which depends on definition and storing of assets generating a Risk Matrix.

To ensure rapid development and compatibility, the following technology stack was selected:

- Django framework for web application development
- MySQL / PostgreSQL database for data storage and management

Basic tool’s capabilities can be summarised as follows:

- Front End with User Interface and API for importing data: provide an intuitive web-based user interface that guides the user into providing the necessary data and presenting results. Also, provide API for file upload and/or integration with other tools.
- Application Logic integrating E-MAF engine: application logic that collects all inputs and using the Risk and Vulnerability libraries applies E-MAF assessment.
- Database for Data storage: storage of Risk and Vulnerability libraries as well as per-user specific information (assets, questionnaire answers, previous results).
- Report engine: the engine can present assessment results as a web page or PDF document.

A basic architecture view of the tool, as described, can also be shown in Figure 36.

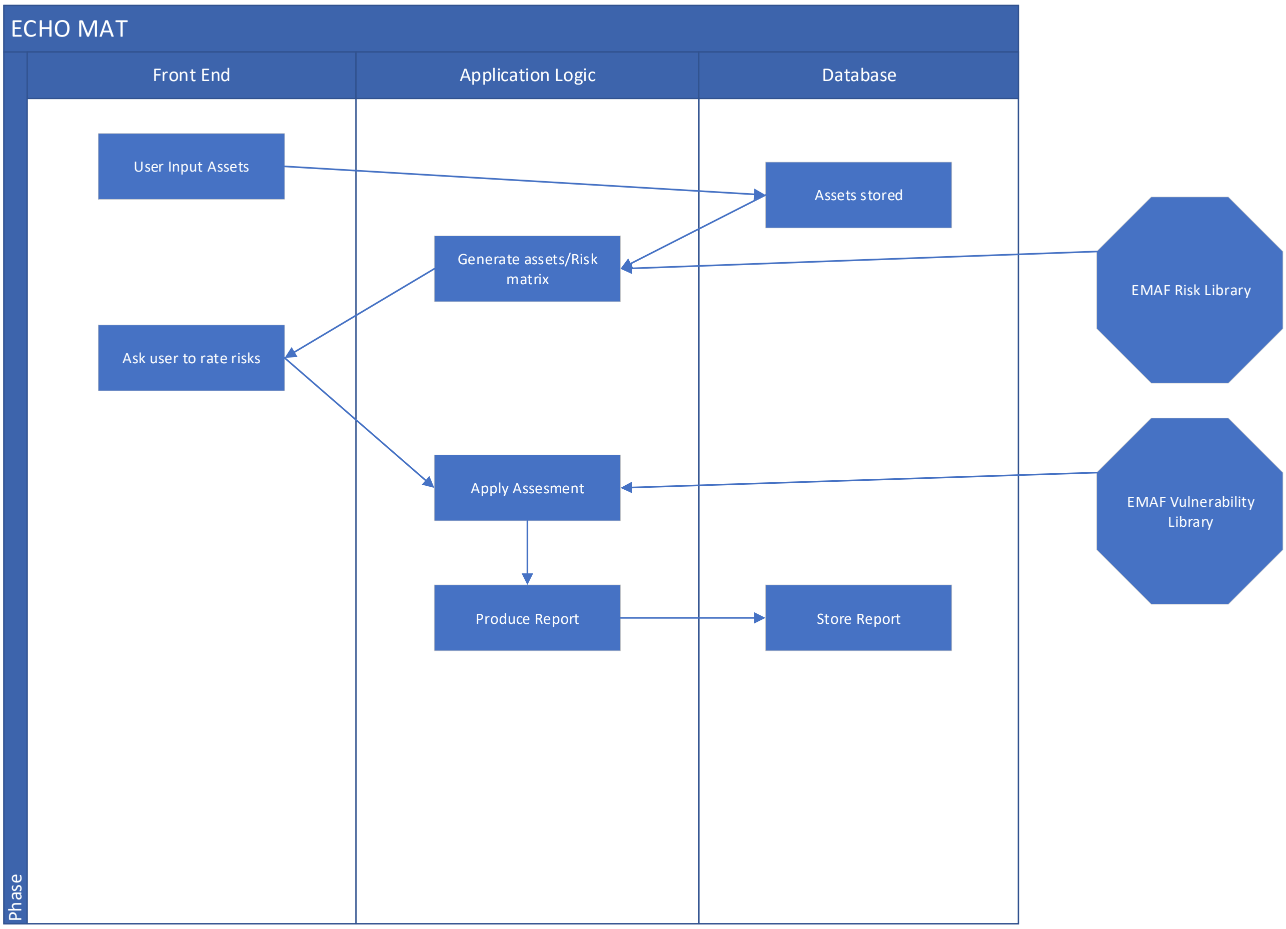


Figure 35: E-MAT workflow.

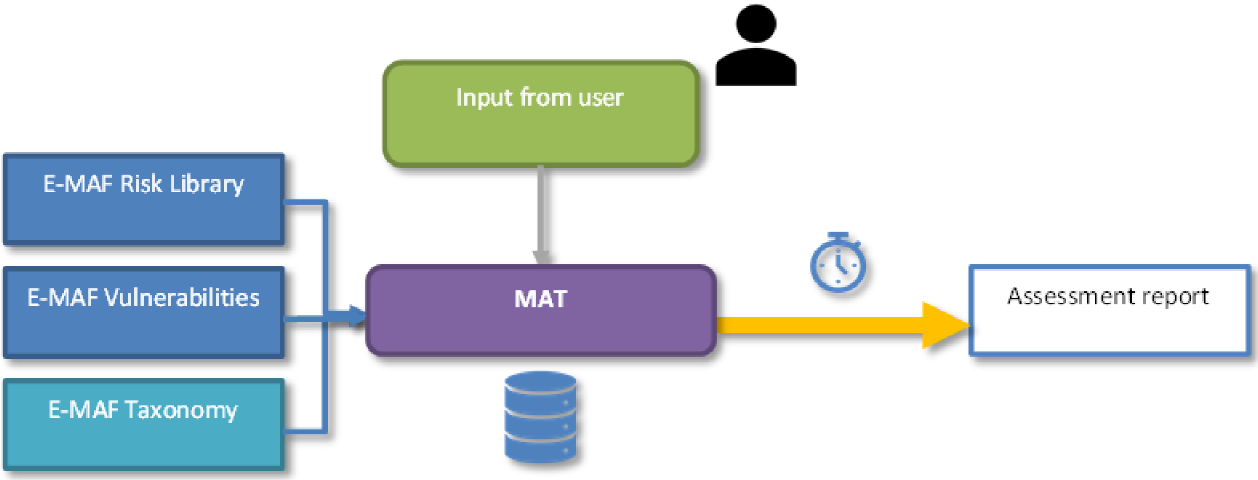
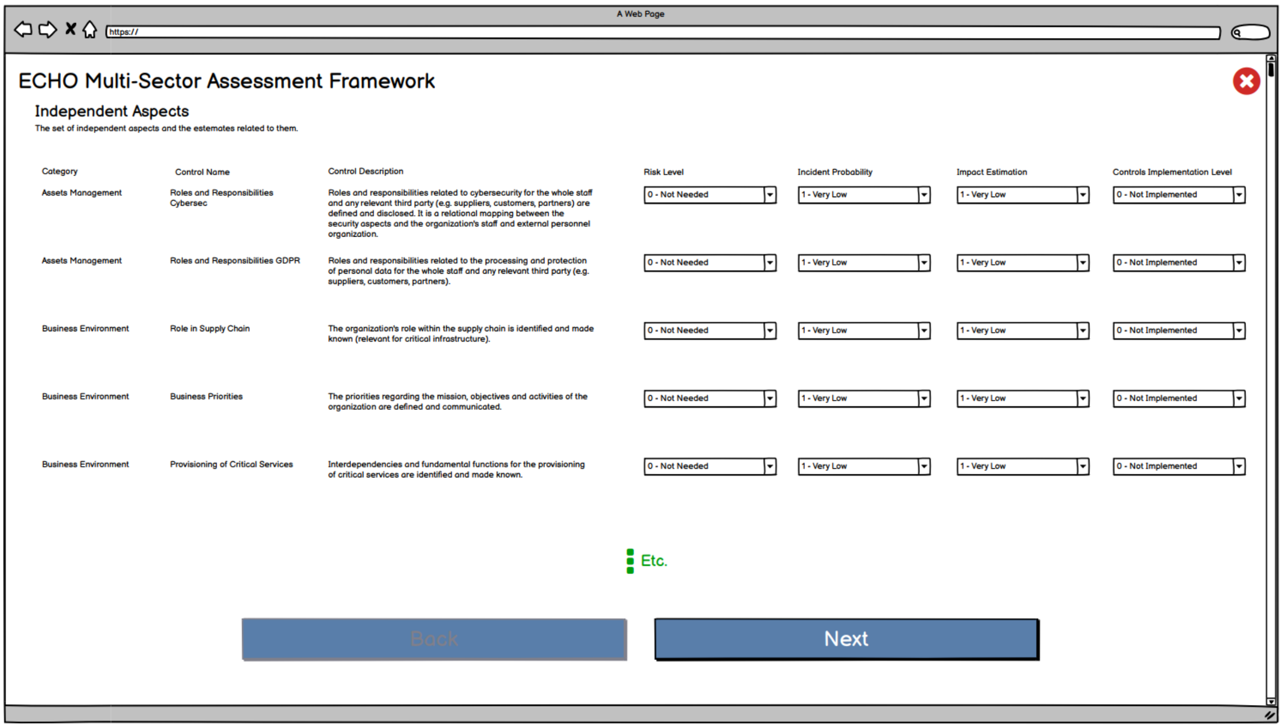


Figure 36: E-MAT architecture.

The graphical user interface from the user's perspective starts from the core of the tool: the whole set of controls included in the questionnaire addressed to the user. As in E-MAF, all controls are divided into categories and sub-categories to better classify the questions and to harmonise the number of controls related to a given area (e.g. maintenance, data security). According to this division, even before detecting the specific controls, the user fails to implement, the output would show the involved categories at a first glance, helping to address the mitigation in a more straight and immediate way. Afterwards, the user may appreciate the single sub-category/control which has a gap. The user is asked to rate each control included in the survey according to a pre-determined scale (0 to 5), where 1 indicates the complete lack of the control implementation, whereas 5 the full one; 0 indicates the control does not apply to the specific organisation. Figure 37 shows a mokup of GUI for Independent issues assessment. Similar ones are foreseen for Transversal, Cross-sector, Multi-sector issues as well.



ECHO Multi-Sector Assessment Framework

Independent Aspects

The set of independent aspects and the estemates related to them.

Category	Control Name	Control Description	Risk Level	Incident Probability	Impact Estimation	Controls Implementation Level
Assets Management	Roles and Responsibilities Cybersec	Roles and responsibilities related to cybersecurity for the whole staff and any relevant third party (e.g. suppliers, customers, partners) are defined and disclosed. It is a relational mapping between the security aspects and the organization's staff and external personnel organization.	0 - Not Needed	1 - Very Low	1 - Very Low	0 - Not Implemented
Assets Management	Roles and Responsibilities GDPR	Roles and responsibilities related to the processing and protection of personal data for the whole staff and any relevant third party (e.g. suppliers, customers, partners).	0 - Not Needed	1 - Very Low	1 - Very Low	0 - Not Implemented
Business Environment	Role in Supply Chain	The organization's role within the supply chain is identified and made known (relevant for critical infrastructure).	0 - Not Needed	1 - Very Low	1 - Very Low	0 - Not Implemented
Business Environment	Business Priorities	The priorities regarding the mission, objectives and activities of the organization are defined and communicated.	0 - Not Needed	1 - Very Low	1 - Very Low	0 - Not Implemented
Business Environment	Provisioning of Critical Services	Interdependencies and fundamental functions for the provisioning of critical services are identified and made known.	0 - Not Needed	1 - Very Low	1 - Very Low	0 - Not Implemented

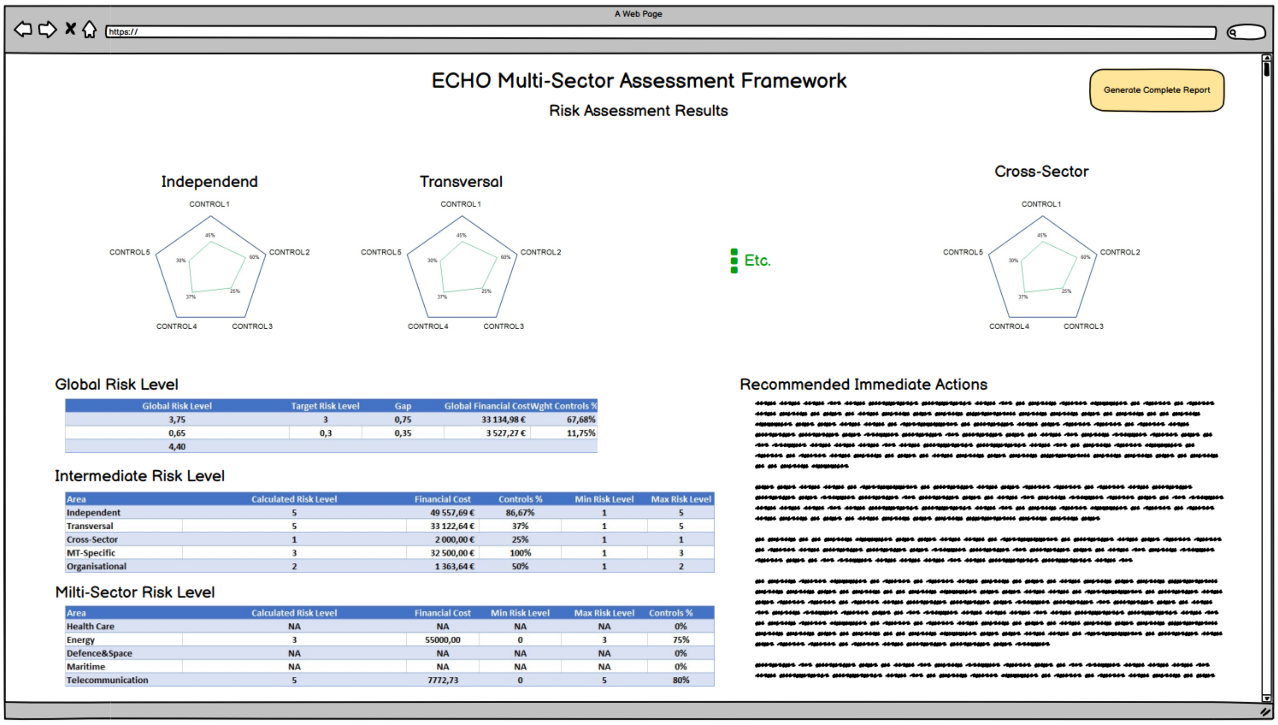
⋮ Etc.

Figure 37: Independent information for the assessment.

Once the input part is completed the output should follow a simple yet complete path, envisaging:

I. classification of categories/ sub-categories where the user is not/ is partially protected;
II. a graphical representation of the gaps in terms of categories/ sub-categories (e.g. columns);
III. mitigation actions provided according to the controls priority ranking;
IV. filtering of the mitigation list due to the gap analysis.

The final result and output should be both written and graphical (see Figure 38). The written part of the document consists of a thorough analysis of the gaps that emerged from the survey, along with a series of mitigation actions. The graphical side of the final output will be highly user-friendly and visually catchy, and it showing almost at a glance where the user has its major gaps according to the security standards.



ECHO Multi-Sector Assessment Framework

Risk Assessment Results

Global Risk Level

Global Risk Level	Target Risk Level	Gap	Global Financial Cost	Wght Controls %
3,75	3	0,75	33 134,98 €	67,68%
0,65	0,3	0,35	3 527,27 €	11,75%
4,40				

Intermediate Risk Level

Area	Calculated Risk Level	Financial Cost	Controls %	Min Risk Level	Max Risk Level
Independent	5	49 557,69 €	86,67%	1	5
Transversal	5	33 122,64 €	37%	1	5
Cross-Sector	1	2 000,00 €	25%	1	1
MT-Specific	3	32 500,00 €	100%	1	3
Organisational	2	1 363,64 €	50%	1	2

Milti-Sector Risk Level

Area	Calculated Risk Level	Financial Cost	Min Risk Level	Max Risk Level	Controls %
Health Care	NA	NA	NA	NA	0%
Energy	3	55000,00	0	3	75%
Defence&Space	NA	NA	NA	NA	0%
Maritime	NA	NA	NA	NA	0%
Telecommunication	5	7772,73	0	5	80%

Recommended Immediate Actions

Figure 38: Radar chart of the set of controls

Description of the Tool Demo

E-MAF and E-MAT (ECHO Multi-sector Assessment Framework and Tool) support the Risk Assessment process in your organisation providing suggestion on mitigation actions to support decision making process in cybersecurity. E-MAF calculates a set of metrics related to organisational cybersecurity posture which depend on the set of esteems provided by the user on the level of implementation and robustness for a set of "cybersecurity controls". You will be requested to provide values in a range 1 to 5 (where 0 represents full lack of implementation for the security control and 5 the optimal implementation for it). You can also use 0 as a value for unnecessary controls for your organisation due e.g. to specific/local operation/situation. On the basis of the values you provide, a global risk level and several intermediate risk levels (per area or per category of controls) will be calculated. The demo will demonstrate how the global risk (and others) related to cybersecurity can be effectively lowered by acting on some controls (e.g. improving staff awareness through cybersecurity training, by promoting smart behaviors, updating software and cybersecurity policies, etc.). The goal of E-MAT demo is to deliver an innovative and graphical approach to enhance comparison between different possible cybersecurity postures within an organizations or among different ones, within a single country or between different ones. The demo will offer usual Use Cases inspired to ones identified by ECHO WP2 (see [D2.1]), preferably relating to different domains among the ones included in ECHO list of domains.

Tool related questions

Question #17.1.E-MAT

How would you esteem the level E-MAT fulfil the need of Risk Assessment providing a way to easy investigate the Cybersecurity posture?

Expected category of answer: **[choice]**

Option list for answer: [Very high
High
Medium
Low
Very low]

If the user replies from "Medium" to "Very high" a textbox appears and a new question is asked:

Question #17.2.E-MAT

Would you consider using this tool in your organisation?

Expected category of answer: **[choice]**

Option list for answer: [Yes, sure
May be
No]

Question #17.3.E-MAT

Would you consider the Risk Assessment provided by E-MAT comparable with any other you ever applied to your organisation?

Expected category of answer: **[choice]**

Option list for answer: [Yes, I see they provide similar values
Yes, but values and risk levels have to be analysed and compared
Yes, but risk levels are very different
May be
No, they can't be compared]

3.1.12 SISP

Description of the Tool

RHEA SISP (Secure Information Sharing Platform) is being developed by RHEA mainly in the scope of the H2020 PANACEA (www.panacearesearch.eu), but some additional adaptation has been provided within ECHO. Being a sector-specific tool solving a set of identified security challenges in healthcare, it has been decided to further develop it in the scope of ECHO and potentially use it for one or more Demonstration Cases.

The goal of SISP is to deliver secure sharing of health care information between different HCO, cross-border and between disparate organisations within a single country. The current approach adopted for exchanging information is using obsolete procedures such as fax, email and exchanging physical medium. The SISP should enable healthcare professionals to exchange healthcare information more efficiently, in compliance with regulations and more securely than the current baseline by promoting interoperable file formats, cryptographic methods and a mutual trust model. The SISP tool will allow HCOs to guarantee the confidentiality, accountability, integrity and availability of the data.

Capabilities

A list of the basic tool's capabilities is shown in the following table.

Category	Functionality	Description	Note
Information sharing	**HC information sharing inter-border**	SISP allows HC information sharing between tenants in the same country, in different HC organizations	
Information sharing	**HC information sharing cross-border**	SISP allows HC information sharing between tenants in different countries (depending on the country, some adaptations to the national laws may be needed)	
Federations management	**Capability to create cross border federations managed at the EU level**	SISP can be completely distributed in federations of tenants: the overall idea is to be able to link multiple HC organizations to the federation to ensure the exchange of data across the continent	
Security	**Confidentiality and integrity of the shared information**	Security-by-design principles have been taken into account during the development of SISP	
Data formats	**Capability to share various HC data formats**	HC sector has a plethora of data formats. SISP is agnostic of the data format and can work with multiple types to ensure compatibility	
Size of shared data	**Capability to share up to 1 GB for a single file**	This is relevant in the case of images or videos	

Table 10: Capabilities of the SISP tool

To implement different trust boundaries between organizations, we developed constituents. The constituents allow us to define which organizations can communicate and establish governance structures over the federation, as shown in Figure 39.

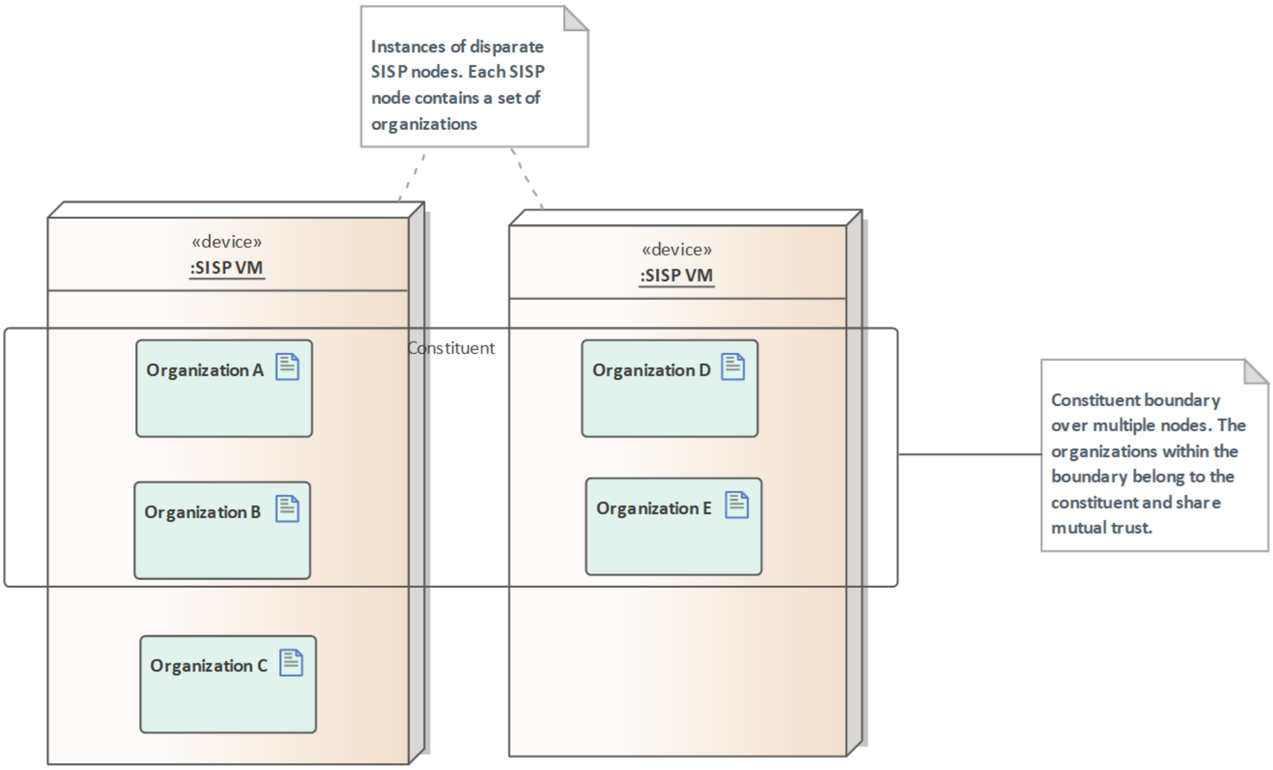

Instances of disparate SISP nodes. Each SISP node contains a set of organizations
«device»
:SISP VM
«device»
:SISP VM
Constituent
Organization A
Organization B
Organization C
Organization D
Organization E
Constituent boundary over multiple nodes. The organizations within the boundary belong to the constituent and share mutual trust.

Figure 39: SISP - Deployment Distributed Multi-Tenant Model

The system can support both a central and a distributed deployment.

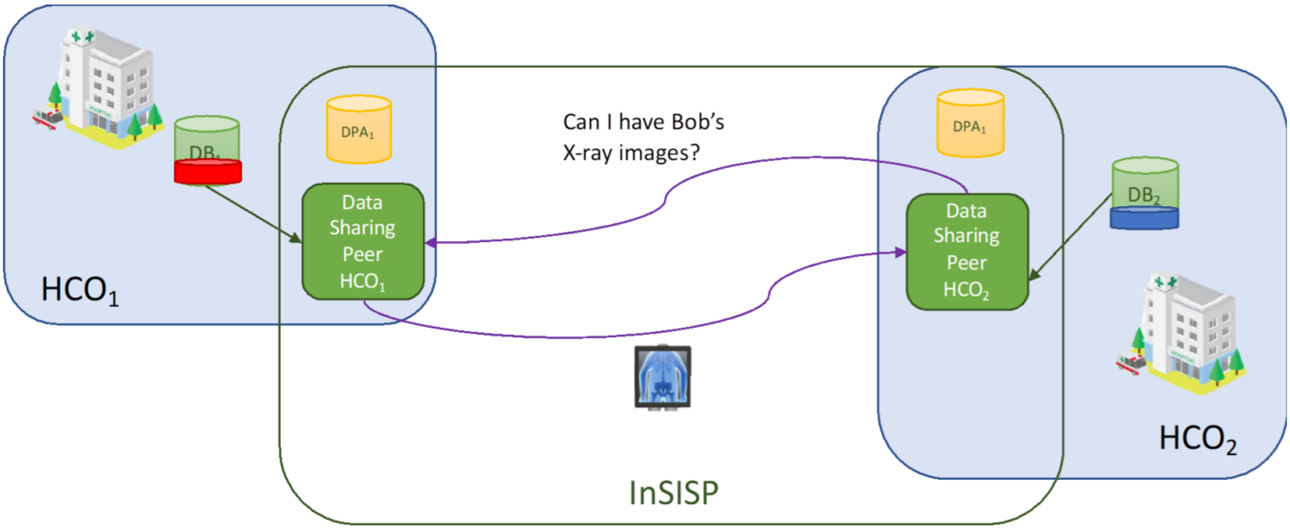


Figure 40: SISP Data Sharing

Other relevant features implemented are the following:

- ability to create an instance of a health care ticket in a different template type, step which allows the user to translate information into a common language or taxonomy

- consent information and data-minimization mitigations to comply with GDPR (for instance, how information might be deleted and also retention for the health information)
- SAML2 interface to support a wide choice of different identity providers
- mechanism for the exchange of large file attachments (SISP can now either store files internally or in external file storage thank to a concrete file storage implementation tested by using MinIO as a file storage service)

Description of the Tool Demo

RHEA SISP (Secure Information Sharing Platform) is a secure sharing support tool, to enhance the cybersecurity of an healthcare organization, enabling healthcare personnel to coordinate and share healthcare information in near-real-time within their own organization and with external organizations (cross-border) more efficiently, in compliance with regulations and more securely than the current baseline (e.g. procedures such as fax, email and exchanging physical medium) by promoting interoperable file formats, cryptographic methods and a mutual trust model. The SISP tool allows Healthcare Organizations to guarantee the confidentiality, accountability, integrity and availability of the data. The goal of SISP is then to deliver secure sharing of health care information between different healthcare organizations, cross-border and between disparate organisations within a single country.

Tool related questions

Question #17.1.SISP

Does the tool reduce the handling time for healthcare information exchange?

Expected category of answer: **[choice]**

Option list for answer: **[Yes,** No]

Il the user replies “No”, a new question appears

If NO, for which reason?

Expected category of answer: **[textbox]**

The rationale is to get a user validation/analysis of the tool compliance to the use case.

Question #17.2.SISP

Do you feel ensured by security offered by SISP?

Expected category of answer: **[choice]**

Option list for answer: **[Yes,** No]

Il the user replies “No”, a new question appears

If NO, what would you like to see improved?

Expected category of answer: **[textbox]**

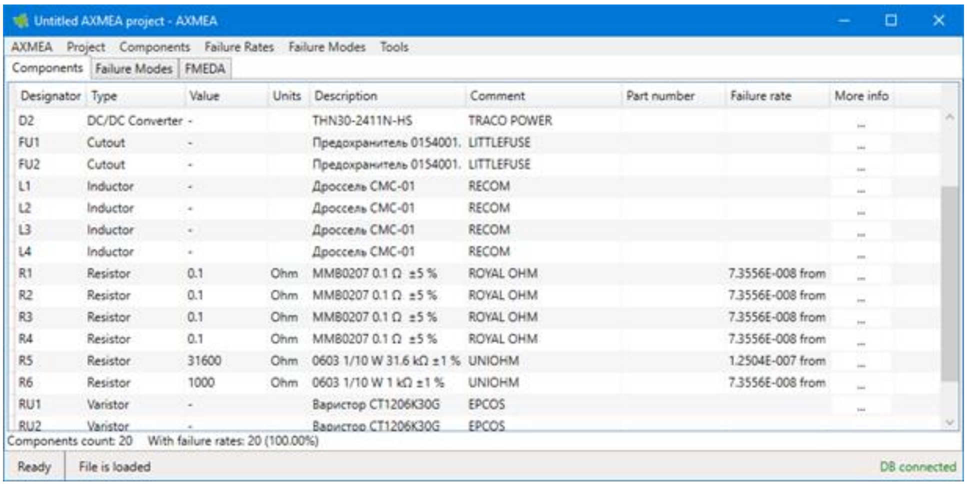
The rationale is to get a user evaluation/perception of the security aspects of the tool.

3.1.13 AXMEA

Description of the Tool

AXMEA tool is used to automate reliability and safety assessment using failure modes, effects, and diagnostic analysis (FMEDA) and providing user possibility to utilize different failure sources, specify their priorities, assign failure rates for electronic components and obtain required safety metrics. Tool is intended to simplify analysis of modern complex electronic products comprising of thousands of different components and minimize influence of expert judgments. AXMEA supports usage of templates for input information (bills of materials etc.) and output information (reports etc.). Database of failure rates of components appropriate to international normative documents is an essential part of AXMEA tool.

All known components are assigned failure rates automatically from different configured failure rate sources (see Figure 72). Database of failure rates is updated cumulatively from project to project.



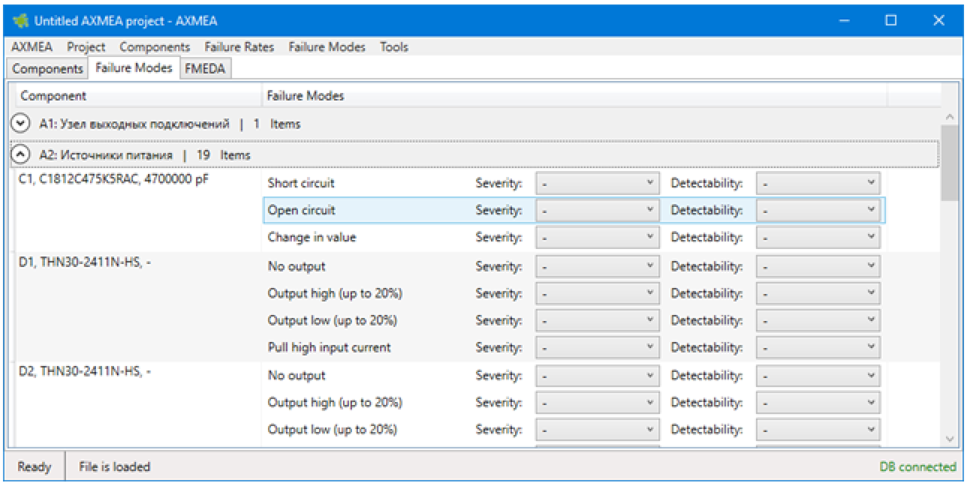
Designator	Type	Value	Units	Description	Comment	Part number	Failure rate	More info
D2	DC/DC Converter	-		THN30-2411N-HS	TRACO POWER			...
FU1	Cutout	-		Предохранитель 0154001.	LITTLEFUSE			...
FU2	Cutout	-		Предохранитель 0154001.	LITTLEFUSE			...
L1	Inductor	-		Дроссель CMC-01	RECOM			...
L2	Inductor	-		Дроссель CMC-01	RECOM			...
L3	Inductor	-		Дроссель CMC-01	RECOM			...
L4	Inductor	-		Дроссель CMC-01	RECOM			...
R1	Resistor	0.1	Ohm	MMB0207 0.1 Ω ±5 %	ROYAL OHM		7.3556E-008 from	...
R2	Resistor	0.1	Ohm	MMB0207 0.1 Ω ±5 %	ROYAL OHM		7.3556E-008 from	...
R3	Resistor	0.1	Ohm	MMB0207 0.1 Ω ±5 %	ROYAL OHM		7.3556E-008 from	...
R4	Resistor	0.1	Ohm	MMB0207 0.1 Ω ±5 %	ROYAL OHM		7.3556E-008 from	...
R5	Resistor	31600	Ohm	0603 1/10 W 31.6 kΩ ±1 %	UNIOHM		1.2504E-007 from	...
R6	Resistor	1000	Ohm	0603 1/10 W 1 kΩ ±1 %	UNIOHM		7.3556E-008 from	...
RU1	Varistor	-		Варистор CT1206K30G	EPCOS			...
RU2	Varistor	-		Варистор CT1206K30G	EPCOS			

Components count: 20 With failure rates: 20 (100.00%)

Ready | File is loaded | DB connected

Figure 72: AXMEA: work with failure rates

Figure 73 shows a tab for working with failure modes. Each component may have one or more failure modes. Each type of failure must be classified according to IEC 61508 as safe detected, safe undetected, dangerous detected, dangerous undetected.


Untitled AXMEA project - AXMEA
AXMEA Project Components Failure Rates Failure Modes Tools
Components Failure Modes FMEDA
Ready
File is loaded
DB connected

Component	Failure Modes				
A1: Узел выходных подключений | 1 Items					
A2: Источники питания | 19 Items					
C1, C1812C475K5RAC, 4700000 pF	Short circuit	Severity:	-	Detectability:	-
	Open circuit	Severity:	-	Detectability:	-
	Change in value	Severity:	-	Detectability:	-
D1, THN30-2411N-HS, -	No output	Severity:	-	Detectability:	-
	Output high (up to 20%)	Severity:	-	Detectability:	-
	Output low (up to 20%)	Severity:	-	Detectability:	-
	Pull high input current	Severity:	-	Detectability:	-
D2, THN30-2411N-HS, -	No output	Severity:	-	Detectability:	-
	Output high (up to 20%)	Severity:	-	Detectability:	-
	Output low (up to 20%)	Severity:	-	Detectability:	-

Figure 73: Assigning of failure types for components

AXMEA provides possibility to generate reports on the work performed. To use report generation functions, an expert must determine the failure rates for all components that were not assigned automatically, as well as their rates and detection/severity, otherwise, one will be notified that not all information is specified to create the table.

Description of the Tool Demo

AXMEA tool automates approaches described in MIL-HDBK-217F, IEC 62380 and other normative documents so as to obtain failure rate for each electronic component basing on its part number, type etc. Classification of failures into safe and dangerous, detected and undetected is supported. Output information are reports generated according to configurable templates. Possibility to work with several projects and the same database of failure rates is provided.

Tool related questions

Question #17.1.AXMEA

What failure rate sources do you usually use during reliability and safety analysis?

Expected category of answer: **[multiple choice and/or text box]**

Option list for answer: [MIL-HDBK-217F
IEC 62380
Bellcore (Telcordia)
RIAC FMD
Other [textbox]]

If the user selects “Other”, a new texbox appears for further specification.

Rationale for this question is to obtain feedback on possible failure rate sources and consider including them in future releases of AXMEA or inform user that their automation is already supported by AXMEA.

Question #17.2.AXMEA

What failure mode sources do you usually use during reliability and safety analysis?

Expected category of answer: **[multiple choice and/or text box]**

Option list for answer: [RIAC FMD
IEC 62061
IEC 61496
IEC 62380
Other [textbox]]

If the user selects "Other", a new texbox appears for further specification.

Rationale for this question is to obtain feedback on possible failure mode sources and consider including them in future releases of AXMEA or inform user that their automation is already supported by AXMEA.

3.2 Cybersecurity challenges addressed by ECHO's Inter-sector prototype tools

A major prerequisite for the selection of the inter-sector prototype tools was for each of them to have a direct link to some of the most critical cybersecurity challenges identified in T4.1 - Detailed analysis of transversal technical cybersecurity challenges. These challenges can be generally categorised as transversal technical cybersecurity challenges (identified and reported in D4.1 - Transversal technical cybersecurity challenges report) and inter-sector technical cybersecurity challenges (identified and reported in D4.2 - Inter-sector technical cybersecurity challenges report). These two categories cover a variety of more specific areas and a wide scope of the cybersecurity domain.

In more detail, transversal and inter-sector cybersecurity challenges emerge from various information technology fields, such as:

- Software and Hardware Security Engineering (Web Applications, Application Security)
- Critical Infrastructure
- IoT, Embedded Systems, Pervasive Systems
- Network and Distributed Systems
- AI and Big Data Analytics
- Data Security and Privacy
- Quantum Technologies
- Incident Handling and Digital Forensics
- Vehicular Systems
- Cloud, Edge and Virtualisation

For every one of these fields a set of technical cybersecurity challenges were identified during the activities of task 4.1 and reported in D4.1 and D4.2 respectively.

In that frame, and in order to cover the most critical cybersecurity challenges, at the beginning of T4.3 Early prototypes selection, research and development, each partner was asked to design and come up with an idea, or even a more mature prototype, covering as much of these challenges as possible and always in line with the specific partner's expertise. The number of challenges addressed, along with the importance of them were also major factors for the final selection of the prototypes to be developed.

Following an extensive selection process, defined and followed during the activities of T4.3, and explained in detail in D4.4 Inter-sector prototypes high-level design, 13 inter-sector prototype tools were selected and are being developed. As presented in Table 4, each of the selected tool attempts to cover multiple transversal and inter-sector technical cybersecurity challenges.

Tool Name (Acronym)	Transversal and Inter-sector Technical Cybersecurity Challenges
Penetration Testing Tool (PT)	• Attribution of cyber-attacks (Challenge matrix ID: 18 • Anomalous events of unknown origin in complex systems • Unauthorized access (Threat ID: 35) • Denial of Service attacks (Threat ID: 58, 67) • Man-in-the-middle attacks (Threat ID: 9, 31) • Configuration and patch management • False positives detecting anomalies, attacks and intrusion attempts (Threat ID: 44) • SQL injection (Threat ID: 41, 54) • Malicious Browser Extensions (Threat ID: 16) • CMS Hacking (Threat ID: 16) • Cross-site scripting / XSS Injection (Threat ID: 33, 41) • Cross-Site Request Forgery (CSRF) (Threat ID :41)
Cyber Threat Intelligence (CTI) Extractor	• Lack of dedicated tools to manage cyber threats (Challenge matrix ID: 16) • Attribution of cyber-attacks (Challenge matrix ID: 18) • Anomalous events of unknown origin in complex systems • False positives in detecting anomalies, attacks and intrusion attempts (Threat ID: 44) • Unauthorized access (Threat ID: 35) • Lack of proper raw data collection (Challenge matrix ID: 21) Other possible challenges: • CMS Hacking (Threat ID: 16) • SQL Injection (Threat ID: 41, 54) • JavaScript Injection (Threat ID: 41) • Attacks on RDP services and Remote Command Execution (Threat ID: 37, 78) • DLL Injections (Threat ID: 38)
Trust & Quality Metrics (TQM)	• Lack of dedicated tools to manage cyber threats (Challenge matrix ID: 16) • Attribution of cyber-attacks (Challenge matrix ID: 18) • Lack of adequate cyber risk mitigation frameworks (Threat ID: 42)

Tool Name (Acronym)	Transversal and Inter-sector Technical Cybersecurity Challenges
SNORT module (SM)	• Brute-force attacks (Threat ID: 33) • Out-of-date security standards and protocols (Threat ID: 3) • Cross-site scripting / xSS Injection (Threat ID: 33, 41) • SQL Injection (Threat ID: 41, 54)
Threat Exposure Calculator (TEC)	• Out-of-date security standards and protocols (Threat ID: 3) • System misconfigurations (Threat ID: 78) • Lack of dedicated tools to manage cyber threats (Challenge matrix ID: 16) • Attribution of cyber-attacks (Challenge matrix ID: 18) • Lack of proper raw data collection (Challenge matrix ID: 21) • Lack of adequate cyber risk mitigation frameworks (Threat ID: 42)
Malware Analysis and Intelligence Tool (MAIT)	• Malware (Threat ID: 34) • Mobile malware (Threat ID: 31, 48), • Malware Anti-Analysis Techniques (Threat ID: 37), • Ransomware (Threat ID: 4, 79) • Lack of adequate cyber risk mitigation frameworks (Threat ID: 42) • Attribution of cyber-attacks (Challenge matrix ID: 18)
Intrusion Detection System Combo (IDS Combo)	Main challenges addressed: • False positives in the detection of anomalies, attacks and intrusion attempts (Threat ID: 44) • Big data security [analytics] (Challenge ID: 8) Other challenges addressed: • 0-day on CPS (Challenge matrix ID: 12) • Anomalous events of unknown origin in complex systems Contributes to resolving the following challenges: • Obfuscation as IDS evasion technique (Threat ID: 6) • Attribution of cyber-attacks (Challenge matrix ID: 18) • Fragmentation as IDS evasion technique (Threat ID: 6) • Flooding as IDS evasion technique (Threat ID: 6)
E-MAF tool (E-MAT)	• Out-of-date security standards and protocols (Threat ID: 3) • System misconfigurations (Threat ID :78) • Lack of cyber situational awareness in national critical infrastructure and gaps in defense-in-depth architecture hacking (Threat ID: 77) • Lack of dedicated tools to manage cyber threats (Challenge matrix ID: 16) • Lack of adequate cyber risk mitigation frameworks (Threat ID: 42) In general addresses vulnerability to multiple issues (e.g. cyber-attacks, system weaknesses, etc.).
Cyber Management System (CyMS)	• Lack of dedicated tools to manage cyber threats (Challenge matrix ID: 16) • Legacy industrial control systems (Threat ID: 22) • Attacks against SCADA systems (Threat ID: 73, 2) • Perimeter defence of ICS/SCADA systems

Tool Name (Acronym)	Transversal and Inter-sector Technical Cybersecurity Challenges
	• System misconfigurations (Threat ID :78) • Mobile Malware (Threat ID: 31, 48) Moreover, associated with IDS, FW, ... and the integration of TrendMicro Manager combined with endpoints address many challenges.
Common Vulnerability Exposure (CVE) Strainer	• Out-of-date security standards and protocols (Threat ID: 3) • Out-of-date and unpatched Windows systems (Threat ID: 14) • Constantly increasing attack surface (Threat ID: 59) • Configuration and patch management in ICS/SCADA
Monitoring System (MonSys)	• Out-of-date security standards and protocols (Threat ID: 3) • Attacks on RDP services and Remote Command Execution (Threat ID: 37, 78) • System misconfigurations (Threat ID :78) • Anomalous events of unknown origin in complex systems • Brute-force attacks (Threat ID: 33)
Secure Information Sharing Platform (SISP)	• Lack of dedicated tools to manage cyber threats (Challenge matrix ID: 16) • Lack of proper raw data collection (Challenge matrix ID: 21) • Attribution of cyber-attacks (Challenge matrix ID: 18) • Gain access to connected medical devices (Threat ID: 73) • Data confidentiality and privacy in cloud environment (Challenge matrix ID: 9) • Big data security (Challenge ID: 8) • Data loss (Threat ID: 44)
Automated X-Modes and Effects Analysis (AXMEA)	• Anomalous behaviour is hard to detect (Threat ID: 61) • Negative effects of complexity and connectivity • False positives detecting anomalies, attacks and intrusion attempts (Threat ID: 44) • Lack of adequate cyber risk mitigation frameworks (Threat ID: 42) • Lack of SCADA/ICS vulnerability assessment tools (Challenge matrix ID: 24) • Hardware vulnerabilities (Threat ID: 47)

Table 11: Transversal and inter-sector technical cybersecurity challenges addressed by the ECHO's inter-sector prototype tools

Since one of the main goals of T8.3 will be to demonstrate and validate the use and innovative aspects of the prototypes, through the realization of tool-specific surveys and/or dedicated workshops, the confirmation of coverage of the initially stated cybersecurity challenges from each tool will serve as a validation method. In that frame, each tool-specific survey will include specific question/s in which the user will validate if the tool in question addresses (partly or fully) each of the initially defined cybersecurity challenges.

4. Conclusions

The objective of the survey is to collect the feedback from the participants of the inter-sector prototypes demonstration events allowing evaluation of prototypes' effectiveness and applicability to the challenge of improving cybersecurity across identified sectors. The feedback will be used to assess further improvements needed and steer the future development of those prototypes.

To ease the submission of the feedback for several prototypes and maximize the usability of the survey, the team decided to create such an elaborated questionnaire, where the training, learning, and providing feedback processes are mixed in a very interesting activities. The survey has been organized in a way that will attract the potential respondents as described in the previous sections.

The key concepts accompanying the survey are:

- General questions are agnostic to the tool and have to be answered only once. Respondent can submit feedback for several prototypes without the overhead of re-entering the survey or repeating the answers;
- To refresh respondents' memory and avoid confusion, links to demonstrative material will be available within the survey;
- The set of Tool-specific questions is answered per each selected tool. The set of questions is dynamically adjusted based on the tools selected;
- Relates to cybersecurity challenges depicted in [D4.1] and [D4.2] and aims to validate tools' effectiveness in terms of addressing those challenges;

At the time of the creation of this deliverable, software development of inter-sector prototypes is still ongoing. Upon the completion of task T4.3 'Early prototypes selection, research and development' in January 2022, tool owners will be asked to prepare the updated media to be incorporated in the survey.

The initial feedback will be taken into consideration to improve the tool's functionalities under task T7.3, 'Early prototypes integration, installation and test', concluding the development of prototypes in July 2022.

All results will be summarized in *D8.5 Completed inter-sector demonstration surveys* in October 2022.

The survey is available here:

https://maynoothpsychology.qualtrics.com/jfe/form/SV_0NA8YpTGSYk86B8