



D7.10

HEIR training for experts and non-experts

Project number	883275
Project acronym	HEIR
Project title	A secure Healthcare Environment for Informatics Resilience
Start date of the project	September 1 st , 2020
Duration	36 months
Programme	H2020-SU-DS-2019

Deliverable type	Report
Deliverable reference no.	D7.10
Workpackage	WP7
Due date	08-2023 – M36
Actual submission date	23/08/2023

Deliverable lead	IMT
Editors	Hervé Debar (IMT)
Contributors	S. Athanassopoulos (HYGEIA), E. Floros (PAGNI), A. Sotiropoulos, A. Alexopoulos (AEGIS), E.Christodoulakis, M. Smyrlis (STS), J. Chang, M. Chang (CUH), A. Zarras (FORTH), Rouven Besters (NSE) <i>Contribution to content of training provided by all HEIR partners.</i>
Reviewers	John Cooper, Karianne Fjeld Lovaas (Noklus)
Dissemination level	PU
Revision	Final
Keywords	Pilots, training, info days

Abstract

Deliverable D7.10 describes the training activities of the HEIR project, organized in April-May 2023 at the project's pilot sites. Each site organized one info-day with two sessions. The non-experts session targeted medical and administrative staff and provided an overview of the HEIR solutions. The IT-experts session targeted IT administrators in hospitals and provided more technical content on the technical solutions. Sessions were generally well received, although improvements could be made on the organization.

Disclaimer

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 content of this document reflects only the author's view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883275

Executive Summary

The HEIR project develops cybersecurity tools and installs them on four pilot sites. The Description of Action indicates that the project will run training sessions for experts and non-experts, to disseminate the technologies developed in the project. To this effect, the HEIR project held four information days, one in each pilot site, including online accessibility. Each of the info days was split in two parts, a training session for non-experts and a training session for IT experts.

The session for non-experts gathered medical and administrative personnel at partners pilot sites. The objective was to raise awareness of cybersecurity issues and showcase the technologies developed in HEIR through videos and examples, in order to facilitate understanding of the technologies and their actual usefulness for medical practitioners. The session concluded with information about cyber hygiene, and practical tips to avoid being compromised by malicious actors. This session had a typical duration of about one hour, and focused on using simple and practical terms and concepts, to avoid confusion.

The session for IT experts gathered IT administrators in hospitals. These personnel have a much better understanding of technology and have potentially already faced cyber threats, so their awareness of the issues solved by HEIR is greater than non-experts. However, cybersecurity is not their main concern, as they are more interested in operations and delivering the services expected by medical and administrative personnel. They may also have a more critical eye on the technologies developed in HEIR, as they are able to understand the benefits, but also the burden that these technologies may introduce, either to themselves or their end users. Sessions had a typical duration of two hours and involved more participation from HEIR technical partners, to provide in-depth description of the technologies.

All sessions concluded with a questionnaire to evaluate the satisfaction of the participants and their perception of the HEIR technologies. Both expert and non-expert participants provided positive feedback about the training sessions and the technologies developed by the HEIR project.

Table of Contents

EXECUTIVE SUMMARY	2
1. INTRODUCTION	4
2. METHODOLOGY	5
2.1 ORGANIZATION OF THE TRAINING	5
2.2 LEARNING OBJECTIVES FOR NON-EXPERTS	5
2.3 LEARNING OBJECTIVES FOR EXPERTS	6
2.4 QUESTIONNAIRE EVALUATION DESCRIPTION	6
3. TRAINING MATERIAL FOR NON-EXPERTS.....	8
3.1 SESSION 1 - INTRODUCTION TO CYBERSECURITY	8
3.2 SESSION 2 - TECHNICAL SESSION AND DEMONSTRATIONS	8
3.3 SESSION 3 - PRACTICAL CYBER-HYGIENE	8
4. TRAINING MATERIAL FOR EXPERTS	9
4.1 INTRODUCTION TO HEIR CONCEPTS	9
4.2 HEIR THREAT HUNTING MODULE	9
4.3 HEIR OBSERVATORY	9
4.4 HEIR PRIVACY-AWARE FRAMEWORK	10
5. TRAINING RESULTS EVALUATION.....	12
5.1 TRAINEE CONSTITUENCY	12
5.2 EVALUATION RESULTS.....	13
6. CONCLUSION	21
7. REFERENCES	22
8. ANNEX 1 – SLIDE DECK FOR NON-EXPERTS	23

List of Figures

FIGURE 1: ASSESSMENT OF CONTENT RELEVANCE TO ROLE/POSITION, OVERALL	13
FIGURE 2: ASSESSMENT OF CONTENT RELEVANCE TO ROLE/POSITION, PER AUDIENCE	14
FIGURE 3: ASSESSMENT OF CONTENT USEFULNESS, OVERALL	14
FIGURE 4: ASSESSMENT OF CONTENT USEFULNESS, PER AUDIENCE	15
FIGURE 5: ASSESSMENT OF EASINESS TO UNDERSTAND CONTENT, OVERALL.....	15
FIGURE 6: ASSESSMENT OF EASINESS TO UNDERSTAND CONTENT, PER AUDIENCE.....	16
FIGURE 7: ASSESSMENT OF EVENT AGAINST EXPECTATIONS, OVERALL	16
FIGURE 8: ASSESSMENT OF EVENT AGAINST EXPECTATIONS, PER AUDIENCE	17
FIGURE 9: ASSESSMENT OF EVENT ORGANIZATION, OVERALL	17
FIGURE 10: ASSESSMENT OF EVENT ORGANIZATION, PER AUDIENCE	18
FIGURE 11: ASSESSMENT OF TOPICS (IT EXPERTS).....	18
FIGURE 12: ASSESSMENT OF TOPICS (NON-IT EXPERTS, ADMINISTRATIVE STAFF)	19
FIGURE 13: ASSESSMENT OF TOPICS (NON-IT EXPERTS, CLINICAL STAFF).....	19
FIGURE 14: SLIDE DECK FOR INTRODUCTION TO CYBERSECURITY	23

List of Tables

TABLE 1: TRAINING PROGRAM FOR NON-EXPERTS	6
TABLE 2: TRAINING PROGRAM FOR EXPERTS	6
TABLE 3: QUALITATIVE FEEDBACK FROM QUESTIONNAIRES.....	20

1. Introduction

This deliverable presents the training and information days carried out at the HEIR pilot sites, to demonstrate the technologies developed in HEIR to all participants, separated between experts (IT personnel essentially) and non-experts (medical or administrative staff, end-users of digital technologies):

The deliverable is structured as follows.

- Section 2 presents the methodology and organization of the training.
- Sections 3 and 4 present the training material used during the sessions, respectively for non-experts and experts.
- Section 5 provides information about the training constituency and evaluation.

2. Methodology

The methodology for the training is as follows:

- We use the technologies provided by HEIR as support for the demonstrations and the training, as it covers most of the areas of cybersecurity we intend to train people in. We include introductory material to support the understanding of non-experts.
- We deliver the training program with the help of the technical partners, to groups of people selected in each of the pilot sites.
- We evaluate the training using questionnaires.

2.1 Organization of the training

The HEIR project has organized dedicated training sessions at its pilot sites (NSE, CUH, PAGNI and HYGEIA) to demonstrate and train the local staff at each organization. The training sessions were all organized in the same way:

- Introduction to cybersecurity (including introduction to the legal aspects)
- Presentation and demonstration of threat hunting
- Presentation and demonstration of the privacy aware framework
- Useful tips
- Evaluation of the session

Each pilot site hosted a training day composed of two sessions. Pilot partners invited their staff and associated employees of their organization, and constituency and the training was delivered with the support of the HEIR technical partners. The sessions for experts and non-experts were clearly separated. Each session was operated in the national language (English for CUH, Norwegian for NSE/Noklus and Greek for HYGEIA and PAGNI). Some sessions were opened for online participation.

2.2 Learning objectives for non-experts

Non expert participants are composed mainly of staff that are carrying out medical or administrative duties within a healthcare organization. These non-expert participants are routinely using the hospital IT infrastructure and may be a target for attackers, particularly in the first steps of an attack, when the attacker seeks to gain a foothold in the IT system.

The proposed cybersecurity training program aims at:

- Raising awareness of the issues regarding cybersecurity in healthcare environments, and provide a basic understanding of the main principles related to cybersecurity: attack motivations and principles, attack concepts, security properties, etc.
- Illustrating through examples hosted by the HEIR demonstration scenarios the attacks and remediations that are available through the HEIR platform.
- Illustrating the framework of data protection, especially medical data, and raising awareness of the threats and possible solutions provided by the HEIR Privacy-Aware Framework.
- Useful tips and advice for working with digital devices and data, in order to limit the risk of such attacks and increase the detection of potential cybersecurity issues.

The proposed organization is as follows:

Timeslot	Speaker	Content
20'	IMT or FORTH	Introduction to cybersecurity. This session will introduce the main concepts related to cybersecurity, explain the origin of cyber-attacks, and introduce useful information for understanding the concepts presented in the HEIR platform.
20'	STS and IBM	Technical session and demonstrations <ul style="list-style-type: none"> - Threat Hunting - Privacy aware framework
10'	IMT, STS or FORTH	Conclusion: practical tips for limiting cyber-risk. This conclusion provides useful tips for limiting the attack surface and practicing a good cyber-hygiene.
10'	Local host	Questionnaire and feedback on training

Table 1: Training program for non-experts

2.3 Learning objectives for experts

Expert participants are made up of IT personnel from the pilot sites. They are responsible for operating the digital infrastructure of the pilots. As such, they are knowledgeable about digital environments and have faced cyberthreats. They therefore have sufficient background to understand the fundamental concepts of the HEIR platform and to provide feedback on the results proposed by our demonstration scenarios.

The HEIR Observatory presentation aims at illustrating the utilization of a cloud-based web application that offers aggregated security related insights across hospitals connected to HEIR ecosystem, thus enhancing the understanding of the hospitals and healthcare organizations security challenges that need to be tackled in order to improve the cybersecurity risk in hospitals.

Timeslot	Speaker	Content
10'	IMT, STS or FORTH	Introduction to the HEIR platform: main concepts, scope and objectives.
20'	BD, STS, SIE, PAGNI	Threat Hunting <ul style="list-style-type: none"> • HEIR Client • HEIR Agent • HEIR Aggregator • Local GUI • RAMA Score
10'	AEGIS, STS	Presentation and demonstration of the HEIR observatory and global RAMA
20'	IBM, WELLICS, NSE, Noklus	Privacy-aware framework PAF demonstration showing three uses cases which were directly inspired by the real-life scenarios in with our Norwegian Healthcare partner.
10'	IMT, STS or FORTH	Conclusion
10'	Local host	Questionnaire and feedback on training

Table 2: Training program for experts

2.4 Questionnaire evaluation description

At the end of each session, participants were requested to fill in an online questionnaire, online or in print.

The questionnaires used are described as part of HEIR Deliverable 6.3, Evaluation and impact analysis[1].

Results of the satisfaction survey are shown in Section 5.2.

3. Training material for non-experts

This section describes the training material for non-experts.

3.1 Session 1 - Introduction to cybersecurity

The objective of this introduction is to ensure that the participants understand the basic concepts of cybersecurity. It consists of two parts, one of which provides examples of recent malicious activity related to the healthcare ecosystem (Not only hospitals, but also pharmaceutical companies), and one which introduces a minimal vocabulary so that participants can understand the main concepts of cybersecurity.

The expected outcome is that participants have been informed about the risks related to digital technologies in healthcare, and that they are able to be better placed to mitigate these attacks.

3.2 Session 2 - Technical session and demonstrations

3.2.1 HEIR Threat Hunting Module

The threat hunting demonstration is provided through a pre-recorded video that includes subtitles and narration in the national language of the HEIR pilots, namely English, Greek, and Norwegian. The video begins by highlighting the current cybersecurity challenges faced in the healthcare environment. It then provides a brief overview of the HEIR solution as a whole before delving into the specifics of the Threat Hunting module and presenting its sub-tools and scores. The video also showcases the two sub-scores, namely the base and temporal, of the Local RAMA scores, along with an explanation of how all the tools and scores collaborate to calculate the Local RAMA score. Additionally, it demonstrates the HEIR aggregator and illustrates how the local RAMA score, and relevant metadata are visualized through the 1st Layer GUI.

3.2.2 Privacy-aware framework

The privacy-aware framework demonstration is delivered using a pre-recorded video, subtitled and narrated in the national language of the participants.

The video not only presents a high-level view of why policy-driven data protection is needed, but also shows, through the use of slides and animations, how the privacy-aware framework can solve data privacy issues relevant in a healthcare environment. A more detailed description of these scenarios is presented in section 4.

3.3 Session 3 - Practical cyber-hygiene

This concluding part aims at providing the participants with the fundamentals of practical cyber-hygiene, as the best course of action to avoid cybersecurity compromise is to train and inform people, both IT professionals and end-users. This section leverages the expertise of HEIR participants to present examples of issues and draw the attention of participants to the mechanisms used by attackers to carry out their attacks.

The section starts with several examples of malicious emails, and presents the features used by attackers to attract the attention of potential victims and entice them into clicking on links or opening attachments. It shows the topics currently used by attackers, and the kind of presentation they use. It includes examples related to service messages, to parcel delivery, or to banks.

The section continues with advice on how to handle digital technologies, avoid information overload that leads to mistakes, advises participants to maintain their digital tools up to date, ensure that they understand authentication mechanisms (to avoid mis-using them), password maintenance, and some information about frequently used security mechanisms.

4. Training material for experts

This section describes the material that was used for the experts training.

4.1 *Introduction to HEIR concepts*

The primary objective of this introduction is to comprehensively acquaint the participants with the fundamental concepts of the HEIR framework. We explore the main components that constitute HEIR, namely the Threat Hunting Module, the Privacy-Aware Framework, and the Observatory. By shedding light on their distinctive roles and functionalities, we aim to provide a deeper understanding of how these elements work synergistically to fortify cybersecurity measures and safeguard data privacy in the healthcare realm.

To augment our discourse, we have thoughtfully prepared a series of presentations and videos that vividly demonstrate the capabilities of the HEIR framework. These materials serve as tangible evidence of the technologies embedded within HEIR, further emphasizing its significance and potential impact.

By the culmination of this session, we believe that all participants will have gained a comprehensive insight into the multifaceted capabilities of the HEIR framework and the technologies it offers. We believe this knowledge will empower them to make informed decisions and contribute effectively to enhancing cybersecurity and data privacy in healthcare environments.

4.2 *HEIR Threat Hunting Module*

Similar to the training material for non-experts, the experts training is provided through a pre-recorded video with subtitles and narration in the national languages of the HEIR pilots: English, Greek, and Norwegian. However, the experts' video includes an additional component—an in-depth technical demonstration of the threat hunting module in HEIR's pilots.

In the first technical demo, the Vulnerability Assessment and Exploit Tester is showcased. This module scans the system, identifies vulnerabilities, and reports them to the Local RAMA calculator. The calculator then calculates the base score of the Local RAMA Score based on the reported issues.

The second video focuses on HEIR's Network Module, which specializes in identifying traffic containing malicious content. Once again, the output from this module is sent to the calculator, which calculates the temporal part of the Local RAMA score.

Detailed outputs of these sub-modules, as well as detected alerts and abnormal activity events from the HEIR's SIEM & Anomaly Detection modules, are visualized and demonstrated through the HEIR's Forensics module (FVT - Forensics Visualization Toolkit) that is accessible via the 1st layer GUI.

Through these technical demonstrations, experts gain a comprehensive understanding of the threat hunting module in HEIR. They witness firsthand how the Vulnerability Assessment and Exploit Tester and the Network Module contribute to identifying vulnerabilities and detecting malicious network traffic, ultimately strengthening cybersecurity measures.

4.3 *HEIR Observatory*

The HEIR Observatory demonstration is delivered through a combination of a slide presentation and a pre-recorded five-minute video. The video is subtitled and narrated in the national language of the participants. This part of the presentation aims to enhance participants' understanding of the security challenges faced by healthcare organizations, that can be tackled via an ecosystem of connected hospitals.

The section begins with the slide presentation providing an overview of the HEIR Observatory. It covers the reasons behind the development of this cloud-based web application, the primary issues related to obtaining security information from health organizations, an analysis of the individuals who would have access to the dashboard, the benefits of utilizing the Observatory, the deployed technologies and the relationship between the HEIR Observatory and the other layers of the HEIR platform.

Following the slide presentation, the video presentation of the HEIR Observatory is shown. It provides an overview of the HEIR ecosystem, a brief description of the Observatory's characteristics, and a demonstration of the 2nd Layer of Visualizations platform. This platform serves as a guide of using the Observatory and accessing the Active Policies of the connected hospitals. The video incorporates slides, animations, and actual screen recordings to explain the aforementioned information.

The first part of the demo presentation focuses on assisting security experts understand how anonymized data and metrics from the local layers of HEIR are visually presented in a meaningful way. In addition, it explores how authorized end-users, such as Regulators or Security Analysts, can access aggregated security relevant knowledge through the dashboard and gain an understanding of the overall security status in healthcare environments.

The second and final part of the demo presentation showcases how authorised users can access the Active Policies of the hospitals connected to the HEIR ecosystem. This enables them to utilize the policies as a knowledge base of cybersecurity rules and regulations.

4.4 HEIR Privacy-aware framework

The Privacy Aware Framework (PAF) work package has produced both a ten-minute non-technical video and a twenty-minute technical video which assumes more expertise in the ICT world.

The video introduces the problem that the Privacy Aware Framework was designed to solve, and presents a high-level, technical overview of the conceptual architecture behind this solution.

Four distinct theoretical scenarios are discussed, all which have arisen from the Norwegian Health Care use case.

The first scenario was directly driven from discussions with the medical practitioners from NOKLUS, who described the difficulties that they have in accessing data from disparate healthcare registries that exist in Norway due to non-automated and locally controlled data access policies. In this use case, the Privacy Aware Framework is able to transparently link these distributed registries, whilst still controlling the access to the aggregated data through policy-driven enforcement.

The second scenario depicted describes how the Privacy Aware Framework can be used to provide fine-grained consent management to patient information, with an example policy showing how consent to patient records can be constrained to a given time period.

In the third scenario, we demonstrate how the export of medical data, collected originally from wearable devices used by people with type 1 diabetes, from FHIR server at a hospital to a secure cloud store (e.g. one accessible by the Diabetes registry) can be controlled by the PAF so that exported data is transformed into anonymous statistical measurements before being released from the FHIR server.

All three of these scenarios are explained in the video both through the use of slides and animations, as well as by actual screen recordings showing both how a user could generate a request for data and the corresponding output from PAF.

The final scenario illustrates the PAF blockchain auditing mechanism which records metadata about data requests. The video shows how these results can be graphically plotted to give more insights about data access patterns.

5. Training results evaluation

This section provides information about the trainee constituency (who was recruited into the training) and how the training was perceived.

5.1 Trainee constituency

5.1.1 PAGNI

Participants in PAGNI included physicians and nurses from all hospital clinical departments, including three intensive care units, as well as administrative and IT personnel. Additionally, IT staff from other hospitals in the Region of Crete were invited and participated in the event successfully. Because they share the same patient medical record platform (PANAKIA), which is Pagni's use case in the project, it was of extra benefit to the invited IT staff.

About 25 people from PAGNI's IT department and other hospitals in the region attended the IT-experts session. About 55 people attended the non-IT staff session, which was primarily attended by doctors and nurses from various departments of PAGNI.

5.1.2 NSE/NOKLUS

The Training Day was held both at the premises of the Nasjonalt senter for e-helseforskning (NSE) and online.

The initial plan was to hold the training in close cooperation with the University Hospital of Northern Norway (UNN). As part of the preparation, key positions within the hospital – namely the cybersecurity department and the department of Clinical Medicine - were contacted and invited to the event. Due to a lack of feedback, the event had to be restructured so that it was no longer held in cooperation with the hospital, but internally at NSE with close support from NOKLUS and the University in Tromsø (UiT).

Two different groups were invited. The first group - non-IT - consisted of four participants with backgrounds from the active nursing and hospital sector and two further participants from the research sector (NOKLUS). The selection of the participants was to ensure that the appropriate background for understanding the project from a medical perspective was given.

For the second part of the event - the IT staff - four participants were invited on site, of which only three were present. Two other participants took part in the online event via the link provided.

The participants were specifically invited because of their expertise in computer science - specialising in machine learning, cyber security, electronic reporting systems and mobile communication for hospitals.

All of the participants also took part in the evaluation of the event afterwards.

5.1.3 CUH

At CUH email invitations was sent to the Trust employees via the communications channels, inviting interested employees to attend. These would be administration, medical and nursing staff that would be non-expert IT professionals, but still use the IT system on a daily basis to perform their duties. Targeted invitations were also sent to the Obstetric Department targeting the medical and midwifery teams that would be expected to use the Team 3 device in their daily work routine – the medical application chosen for the CUH Use case demonstration.

For the technical staff, then posters, as well as personal invitations were sent to the IT Department, inviting the managers responsible for maintaining the IT structure, including Firewalls and IT security, to attend and provide feedback on the ease of use, as well as usability

and usefulness of the HEIR platform and associated tools. Furthermore, they were in a position to be able to evaluate how HEIR compares to the products already being used within the Trust. For the IT staff, 6 persons attended, 4 physically and 2 via teams. For the non-IT staff, 10 persons attended, 3 physically and 7 via teams.

5.1.4 HYGEIA

For the best possible feedback, the hospital selectively invited experts to attend the two sections of the training day. Specifically:

- IT Experts: All the IT staff of the hospitals and other companies belonging to the Hellenic HealthCare Group were invited. Seventeen (17) attended the relevant section, most of them in person.
- Non-IT Experts: For the non-IT section, the invitation was sent only to management staff, administrative and clinical, to ensure that the feedback would come from those who have many years of experience in different roles/positions, but also be able to influence any decision on future use of the HEIR platform. Fifteen (15) attended the relevant section, most of them in person.

Although the responses to the questionnaires were anonymous, given the dates they were received, we estimate that approximately thirty (30) of the participants in the HYGEIA training day responded to the questionnaires.

5.2 Evaluation results

This section evaluates the satisfaction of the training participants with the proposed content developed for experts and non-experts.

Q: How relevant was the content to your role and/or position?

R: Responses were in the form of a Likert scale, ranging from 1 (not relevant) to 5 (very relevant). Results are shown in Figure 1.

Out of **68** respondents, only **11 (16%)** considered that the content of the presentations was not the most appropriate for their role/position, while **43 (63%)** considered quite the opposite.

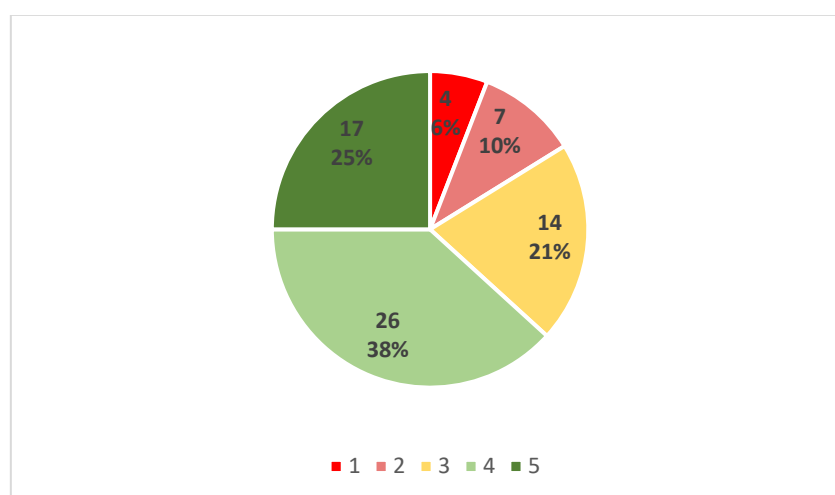


Figure 1: Assessment of content relevance to role/position, overall

Figure 2 presents the same information, adding in it the split between administrative, clinical and IT staff. The first two categories are non-IT specialists. The split between

categories uses small horizontal bars (for Administrative), checkerboard (for Clinical) and plain (for IT staff) overlays on the graph bars.

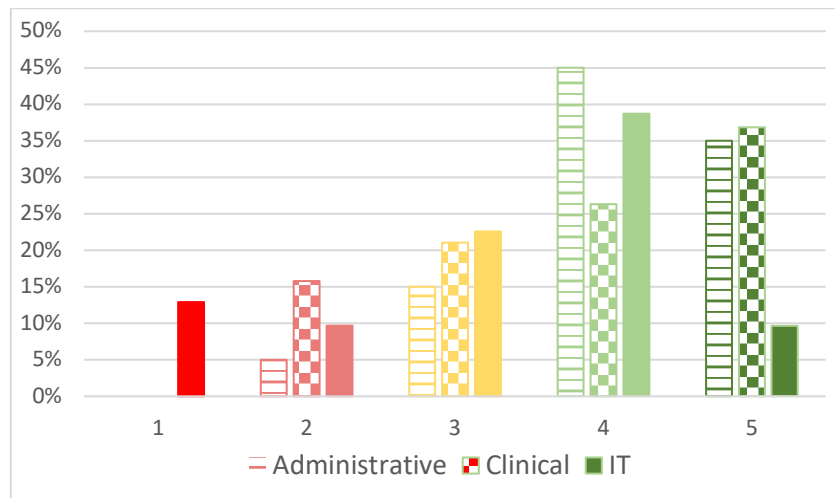


Figure 2: Assessment of content relevance to role/position, per audience

As shown in both figures, satisfaction was rather high. We should note the discrepancy observed for the IT staff, at the lowest (1) and highest (5) values of the scale, which we hypothesize that can be attributed to better familiarity with technical content and so more confidence in formulating a clear opinion.

Q: How useful was the content?

R: Responses were in the form of a Likert scale, ranging from 1 (not useful) to 5 (very useful). Results are shown in Figure 3.

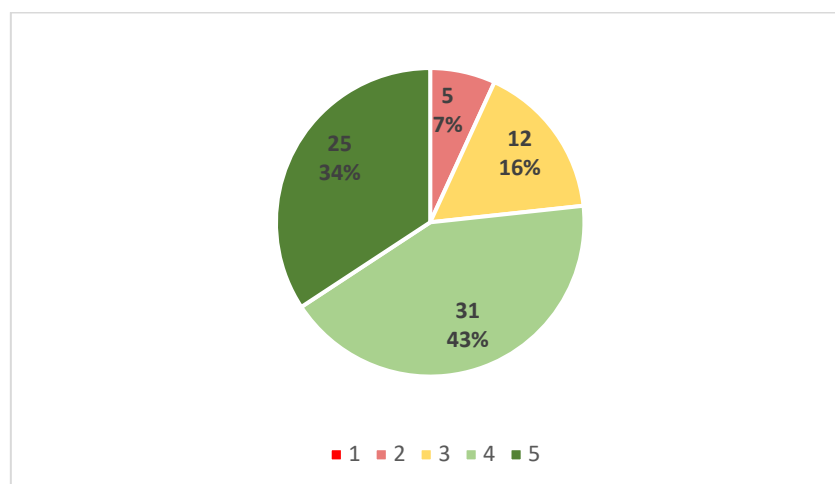


Figure 3: Assessment of content usefulness, overall

Out of 73 respondents, a vast majority of 56 (77%), rate the content as useful or very useful, a fairly positive result. No noteworthy discrepancies between audiences were observed.

Figure 4 provides a more detailed distribution between Administrative (horizontal fine lines style), Clinical (checkerboard style) and IT staff (plain style).

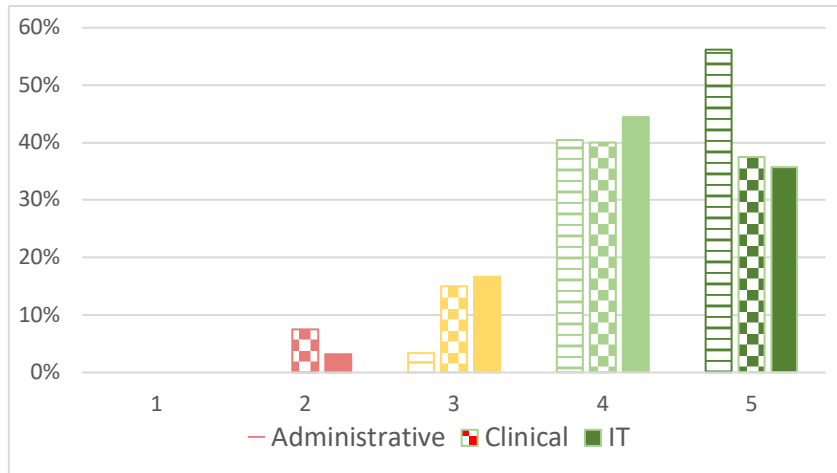


Figure 4: Assessment of content usefulness, per audience

Figure 4 again shows that content appreciation is again slightly more critical for IT staff.

Q: Was the training easy to understand?

R: Responses were in the form of a Likert scale, ranging from 1 (not easy) to 5 (very easy).

As shown in Figure 5, we received a very good rating for this question also, since out of 72 respondents, 50 (70%), found the content easy or very easy to understand.

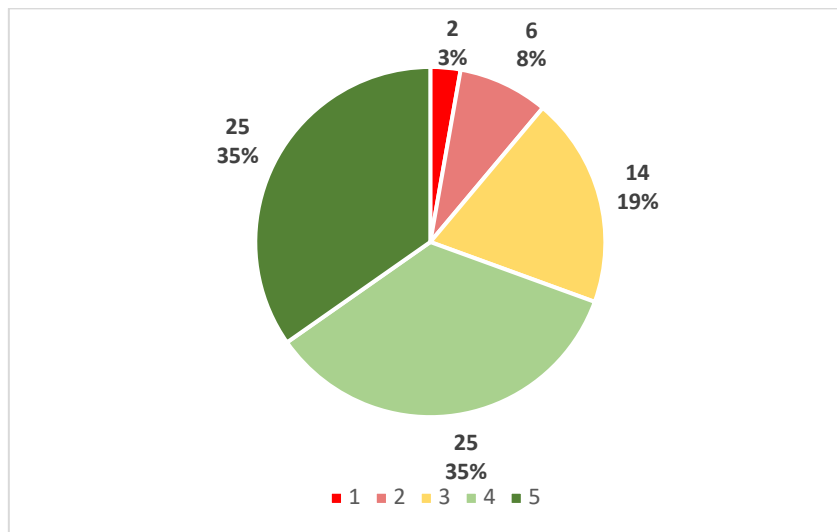


Figure 5: Assessment of easiness to understand content, overall

Figure 6 provides a more detailed distribution between Administrative (horizontal fine lines style), Clinical (checkerboard style) and IT staff (plain style).

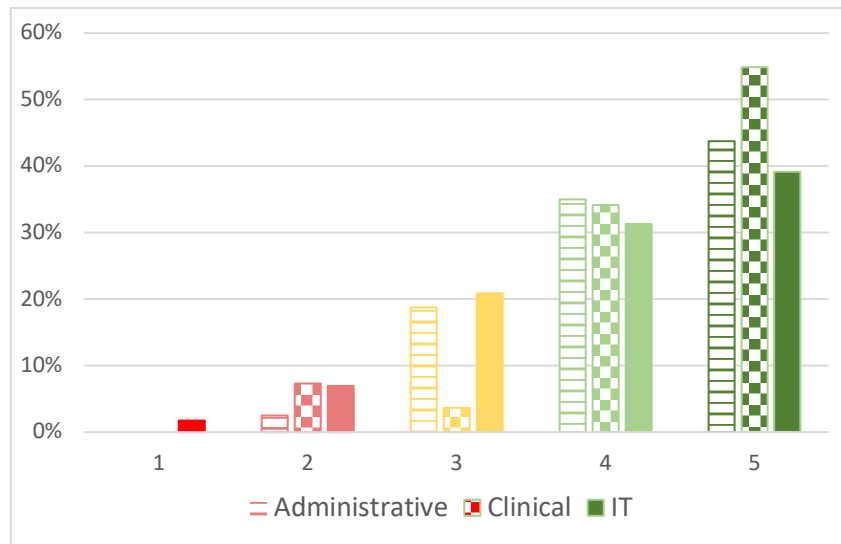


Figure 6: Assessment of easiness to understand content, per audience

No noteworthy discrepancies between audiences were observed.

Q: How would you rate this event compared to your expectations?

R: Responses were in the form of a Likert scale, ranging from 1 (less than expected) to 5 (exceed expectations).

In Figure 7, positive responses (rate 4 or 5) account for **53%** (**39** out of **73** respondents), while negative ones only **8%**. Rate 3 gathered **38%**, allowing for further tailoring of the event, with relevant suggestions to be traced in the last of this set of questions.

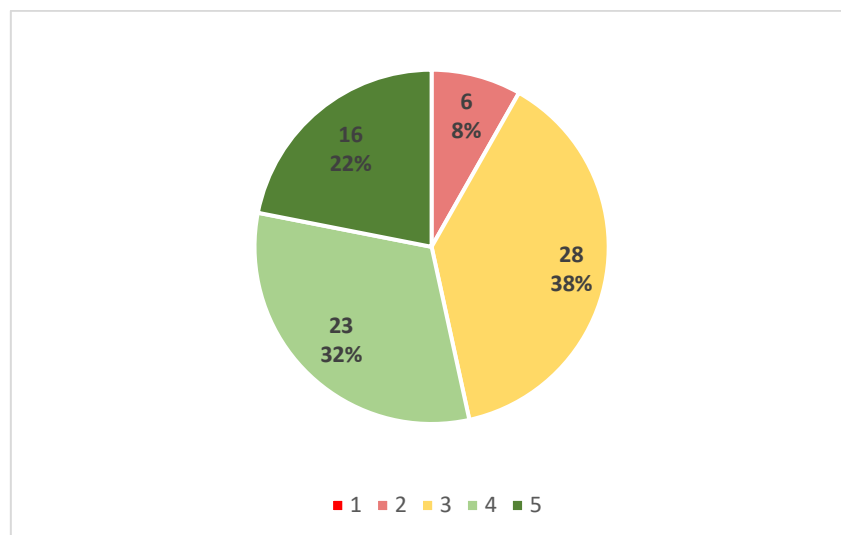


Figure 7: Assessment of event against expectations, overall

Figure 8 provides a more detailed distribution between Administrative (horizontal fine lines style), Clinical (checkerboard style) and IT staff (plain style).

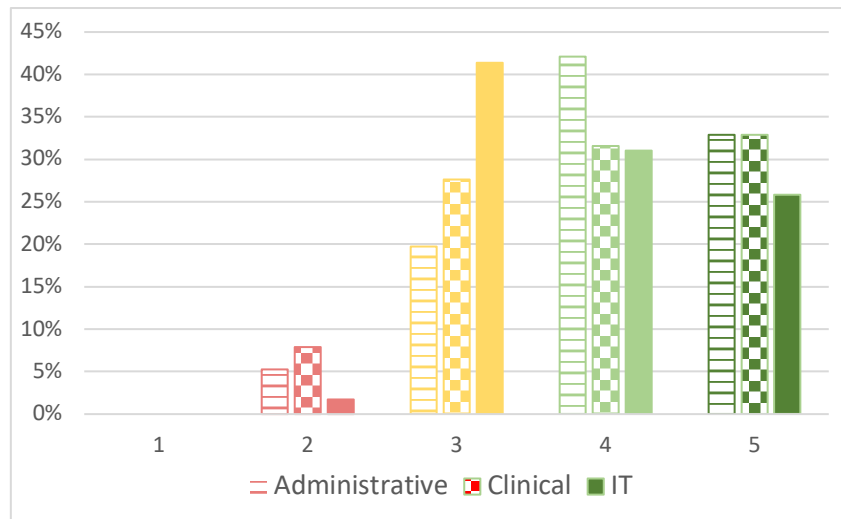


Figure 8: Assessment of event against expectations, per audience

No noteworthy discrepancies between audiences were observed.

Q: How well organized was the event?

R: Responses were in the form of a Likert scale, ranging from 1 (poorly organized) to 5 (very well organized).

The responses in Figure 9 reveal a very successful organization of the training days, since a remarkable **77%** of the respondents (55 out of 72), rate the organization as well organized or very well organized.

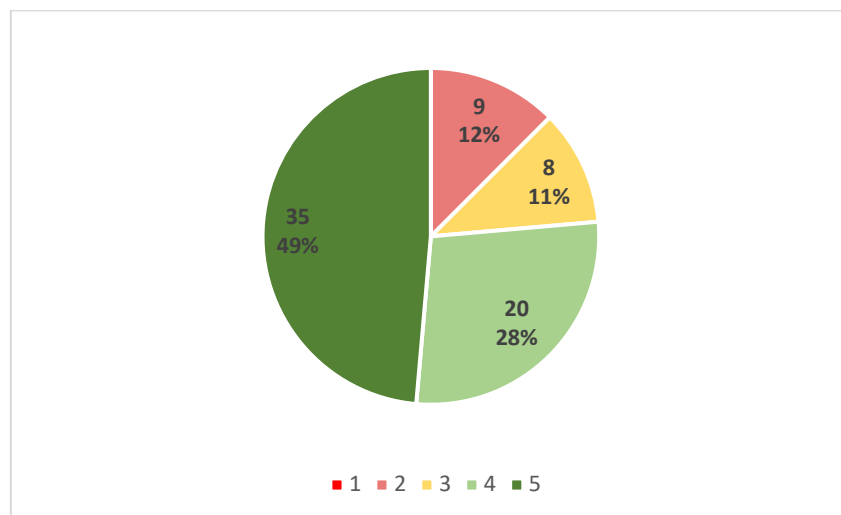


Figure 9: Assessment of event organization, overall

Figure 10 provides a more detailed distribution between Administrative (horizontal fine lines style), Clinical (checkerboard style) and IT staff (plain style).

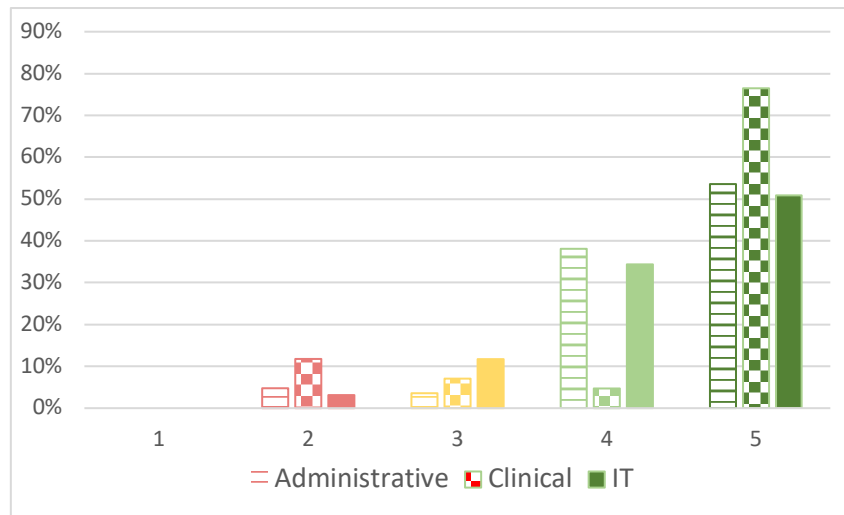


Figure 10: Assessment of event organization, per audience

No noteworthy discrepancies between audiences were observed.

Q: Which topics do you consider as the most interesting and which ones as the least interesting?

R: This question asks participants to rate - in terms of interest - the topics presented. Responses were in the form of a Likert scale, ranging from 1 (least interesting) to 5 (most interesting). As the topics were different for IT and non-IT experts (Administrative and Clinical staff), the responses are presented separately below.

- **IT experts (Figure 11):** All 5 topics seem to have intrigued the participants, with a slight preference for those referring to the most technically demanding elements, namely the Anomaly Detection Module and the Privacy Aware Framework.

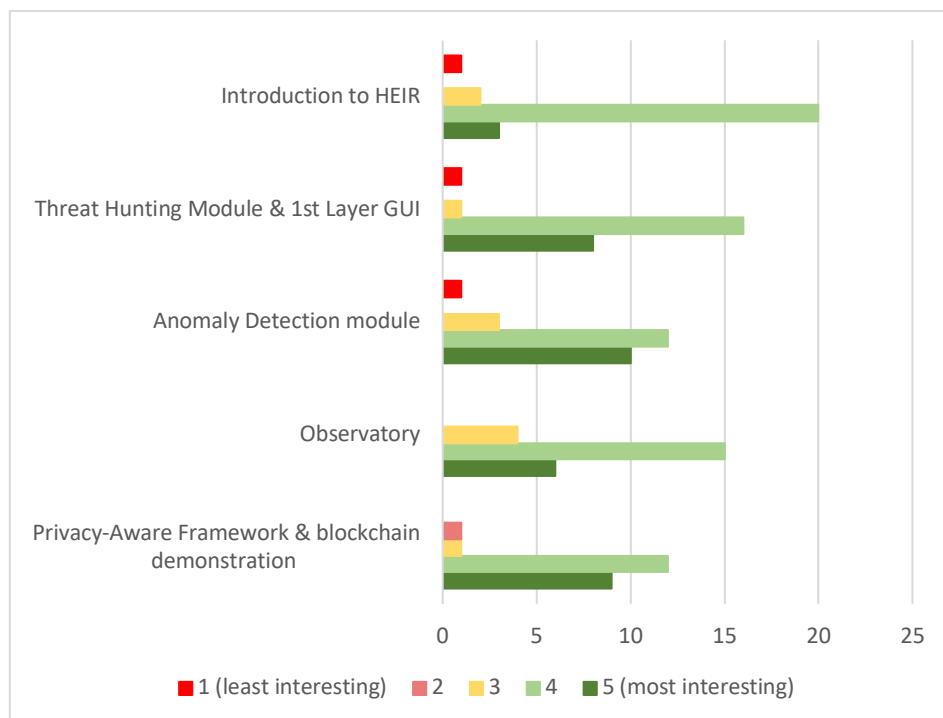


Figure 11: Assessment of topics (IT experts)

- **Non-IT experts (Administrative staff - Figure 12):** All 4 topics were also very well received, surprisingly so for the most technical ones, indicating that the presentations were optimally tailored to this audience.

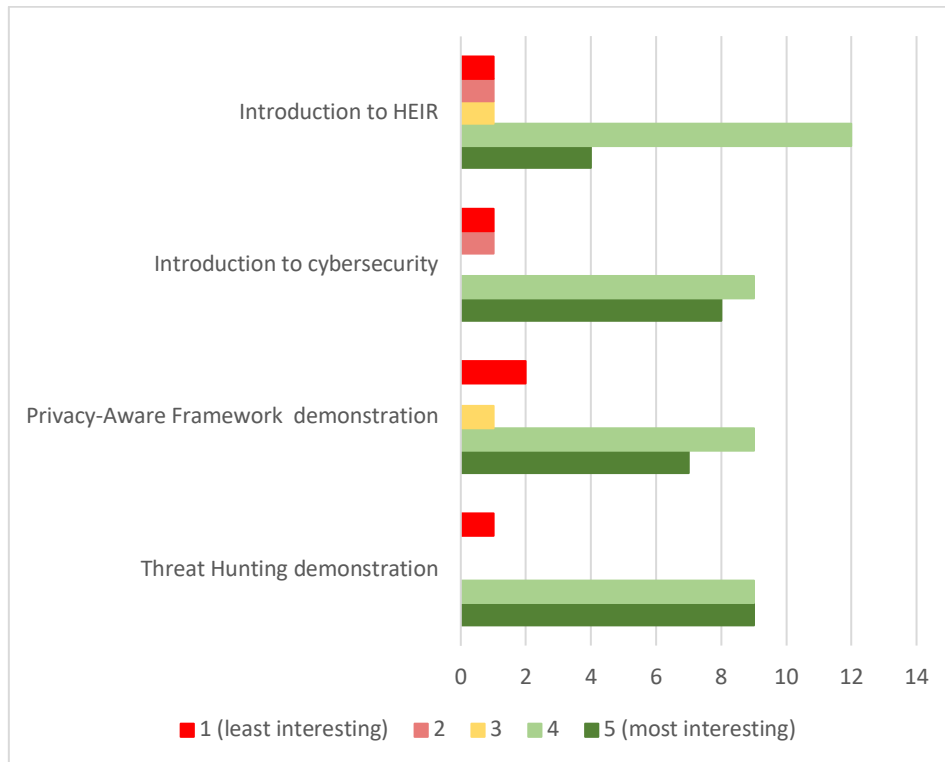


Figure 12: Assessment of topics (non-IT experts, Administrative staff)

- **Non-IT experts (Clinical staff - Figure 13):** Same conclusions as for the Administrative staff.

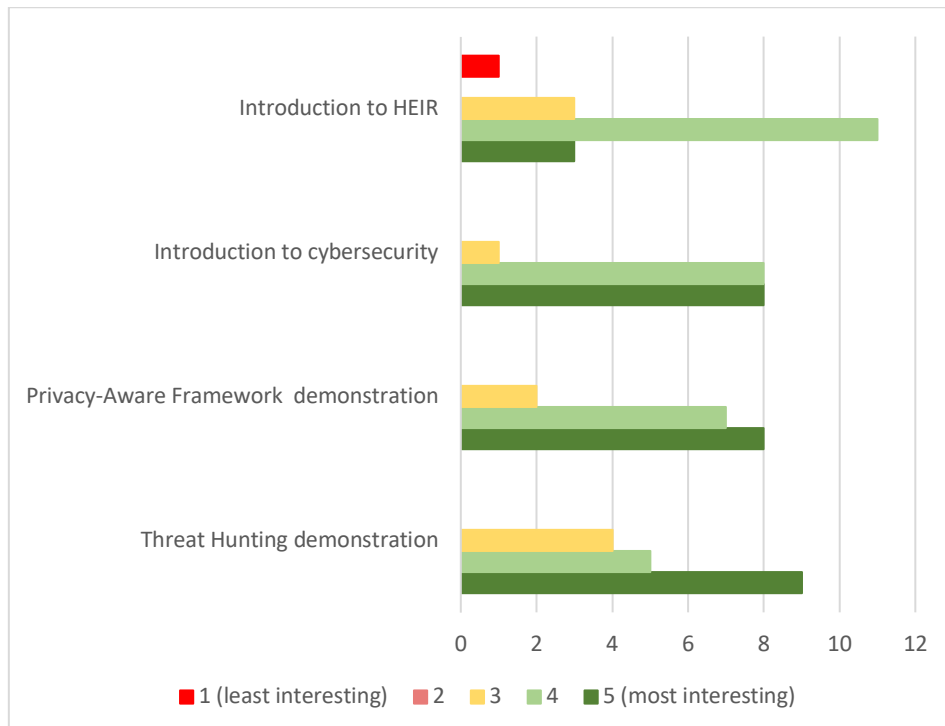


Figure 13: Assessment of topics (non-IT experts, Clinical staff)

As a final note to this question, the topic "Introduction to HEIR" seems to receive proportionally the fewest "most interesting" responses, which can be interpreted as leaving some room for improvement for this presentation.

Q: How do you think the event could have been improved?

R: This was the only open-ended question in this set. Responses were anticipated from all participants, the ones provided are listed below:

Audience	Response
Administrative	Nothing
Administrative	More interactive. Analyze more some case studies relevant to the subject.
Administrative	Include more examples of how to avoid threats, propose smart solutions and be less technical
Clinical	Less technical aspects
Clinical	Less technical for the Privacy Aware Framework and more examples.
Clinical	Not know
Clinical	Less of IT-language, even if you tried to make it easy to understand it was somewhat difficult to follow during the presentation. The video presentation was the hardest to understand, the one presenting in the meeting was easier.
Clinical	Keep the time
Clinical	For average clinicians it should be much more simplified, it is very difficult to understand, for me at least. Except from the part with e-mail threats and the importance of eks 2- factor authenticators- that was useful. It was a bit chaotic at start due to the lack of one of the presenters, but the one who took over and provided the lectures was very good and I am impressed of his performance:-)
Clinical	Bigger screens
IT	Yes, less in more. For such a short time, there was quite a lot of details that could have been abstracted from, and some abbreviations that could have been expanded before using.
IT	The content of the event was too dense with too much information. In addition, the information was not easy to understand, and the event was too long and difficult to follow. For example, I do not see the point of showing lines of code that you cannot even read.
IT	Smoother transition between segments
IT	More room for mingling
IT	I would like to have a list of terminology and abbreviation explanations.
IT	Demo of system if possible.
IT	Be extended in time and have more time for discussions.
IT	AI

Table 3: Qualitative feedback from questionnaires

From these responses, three points for improvement are deduced:

- A common request from all three audiences, and especially from the clinical staff, is for less technical details and simplification of the content, that at some points was difficult to follow.
- More examples/case studies are also considered to improve the overall perception of the topics presented.
- The event could become more interactive, providing time for discussions and audience engagement.

6. Conclusion

As indicated in the description of action, the HEIR project has organized info-days (for non experts) and training sessions (for IT experts) at pilot sites. This has culminated in the development of slide decks and training videos of the HEIR technologies for dissemination purposes.

The infodays were held both physically at pilots' premises and were accessible online to facilitate attendance as well as remain a source of training material for future review by staff on an ad-hoc basis as needed. The training sessions gathered about 140 people, either physically present in training rooms (about 50%) and the others remotely. The videos describing the technical components have been published on HEIR's youtube channel¹ and will remain available.

The analysis of the 68 questionnaires collected at the end of the sessions (about 50% return rate) demonstrate that the majority of participants appreciated the event and learned useful information about the topics developed in HEIR. Despite the organization cost to the project, these events have clearly proven successful and useful, and similar cybersecurity-related events could be organized in healthcare facilities to raise awareness and improve cybersecurity incident response.

¹ https://www.youtube.com/channel/UC_boW9_ifvcZxNpbSIQ8acw

7. References

[1] HEIR Consortium, “HEIR Deliverable 6.3 - Evaluation and impact analysis,” Aug. 2023.

8. Annex 1 – Slide deck for non-experts

This section provides the slide deck used for the non-experts training session. This slide deck is completed by two videos that are shown at the placeholders identified in the slide deck for the threat hunting and privacy aware framework.

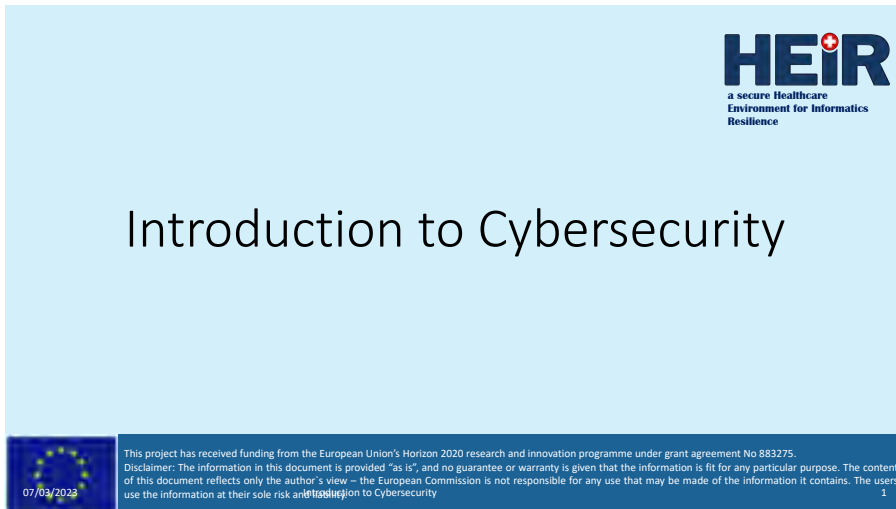


Figure 14: Slide deck for introduction to cybersecurity



Also in the healthcare ecosystem



CPO HOME NEWS INSIGHTS RESOURCES

Fourth-Largest Generic Drugs Manufacturer Sun Pharmaceuticals Hit by Ransomware Attack

The world's fourth-largest generic drugs manufacturer Sun Pharmaceuticals disclosed a ransomware attack that compromised some of its IT systems. The Mumbai-based drugmaker restored the impacted IT systems after detecting an "information security incident" resulting in the "breach of certain file systems and the theft of certain company data and personal data."

"This is an advisory [only] that an information security incident has occurred at the Company and the impacted IT assets have been isolated," Sun wrote in a [Tuesday Slack Exchange filing](#).

Cybersecurity Alerts & Advisories

[View Cybersecurity Advisories List](#)

- 2023-03-02 - 0:00 (CVE-2023-0301) - **B. Braun Bactera Pack SP with Wi-Fi**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **Medtronic Micro Clinician and InterSim Apps**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **ID Alarm Infection Control (Subdate A)**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **Philips Patient Information Center (X, PDC) (X) and Efflica CM Series (Subdate A)**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **ID BodyGuard Pumps**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **Hillrom Medical Device Management (Subdate C)**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **AlereCor KardiaMobile**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **B. Braun SpaccCon, Bactera Pack SP with Wi-Fi, and Data module connectica (Subdate A)**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **B. Braun InfectionCare Large Volume Pump (Subdate A)**
- 2023-03-02 - 0:00 (CVE-2023-0300) - **ID Toleris MultiProcessor**

Medical advisories

1. EXECUTIVE SUMMARY

- CVE-2023-0302
- ATTENTION: PoC exploit available
- Vendor: Bactera Pack SP with Wi-Fi
- Exploit: Remote Ransomware (Subdate B)
- Exploit: Remote Ransomware (Subdate C)
- Exploit: Remote Ransomware (Subdate D)
- Exploit: Remote Ransomware (Subdate E)
- Exploit: Remote Ransomware (Subdate F)
- Exploit: Remote Ransomware (Subdate G)
- Exploit: Remote Ransomware (Subdate H)
- Exploit: Remote Ransomware (Subdate I)
- Exploit: Remote Ransomware (Subdate J)
- Exploit: Remote Ransomware (Subdate K)
- Exploit: Remote Ransomware (Subdate L)
- Exploit: Remote Ransomware (Subdate M)
- Exploit: Remote Ransomware (Subdate N)
- Exploit: Remote Ransomware (Subdate O)
- Exploit: Remote Ransomware (Subdate P)
- Exploit: Remote Ransomware (Subdate Q)
- Exploit: Remote Ransomware (Subdate R)
- Exploit: Remote Ransomware (Subdate S)
- Exploit: Remote Ransomware (Subdate T)
- Exploit: Remote Ransomware (Subdate U)
- Exploit: Remote Ransomware (Subdate V)
- Exploit: Remote Ransomware (Subdate W)
- Exploit: Remote Ransomware (Subdate X)
- Exploit: Remote Ransomware (Subdate Y)
- Exploit: Remote Ransomware (Subdate Z)

1. EXECUTIVE SUMMARY

- CVE-2023-0302
- Vendor: Bactera Pack SP with Wi-Fi
- Exploit: Remote Ransomware (Subdate B)
- Exploit: Remote Ransomware (Subdate C)
- Exploit: Remote Ransomware (Subdate D)
- Exploit: Remote Ransomware (Subdate E)
- Exploit: Remote Ransomware (Subdate F)
- Exploit: Remote Ransomware (Subdate G)
- Exploit: Remote Ransomware (Subdate H)
- Exploit: Remote Ransomware (Subdate I)
- Exploit: Remote Ransomware (Subdate J)
- Exploit: Remote Ransomware (Subdate K)
- Exploit: Remote Ransomware (Subdate L)
- Exploit: Remote Ransomware (Subdate M)
- Exploit: Remote Ransomware (Subdate N)
- Exploit: Remote Ransomware (Subdate O)
- Exploit: Remote Ransomware (Subdate P)
- Exploit: Remote Ransomware (Subdate Q)
- Exploit: Remote Ransomware (Subdate R)
- Exploit: Remote Ransomware (Subdate S)
- Exploit: Remote Ransomware (Subdate T)
- Exploit: Remote Ransomware (Subdate U)
- Exploit: Remote Ransomware (Subdate V)
- Exploit: Remote Ransomware (Subdate W)
- Exploit: Remote Ransomware (Subdate X)
- Exploit: Remote Ransomware (Subdate Y)
- Exploit: Remote Ransomware (Subdate Z)

1. EXECUTIVE SUMMARY

- CVE-2023-0302
- ATTENTION: PoC exploit available, the attack complexity is low
- Vendor: Bactera Pack SP with Wi-Fi
- Exploit: Remote Ransomware (Subdate B)
- Exploit: Remote Ransomware (Subdate C)
- Exploit: Remote Ransomware (Subdate D)
- Exploit: Remote Ransomware (Subdate E)
- Exploit: Remote Ransomware (Subdate F)
- Exploit: Remote Ransomware (Subdate G)
- Exploit: Remote Ransomware (Subdate H)
- Exploit: Remote Ransomware (Subdate I)
- Exploit: Remote Ransomware (Subdate J)
- Exploit: Remote Ransomware (Subdate K)
- Exploit: Remote Ransomware (Subdate L)
- Exploit: Remote Ransomware (Subdate M)
- Exploit: Remote Ransomware (Subdate N)
- Exploit: Remote Ransomware (Subdate O)
- Exploit: Remote Ransomware (Subdate P)
- Exploit: Remote Ransomware (Subdate Q)
- Exploit: Remote Ransomware (Subdate R)
- Exploit: Remote Ransomware (Subdate S)
- Exploit: Remote Ransomware (Subdate T)
- Exploit: Remote Ransomware (Subdate U)
- Exploit: Remote Ransomware (Subdate V)
- Exploit: Remote Ransomware (Subdate W)
- Exploit: Remote Ransomware (Subdate X)
- Exploit: Remote Ransomware (Subdate Y)
- Exploit: Remote Ransomware (Subdate Z)

Incidents in the UK



Mediatechive

75% of infusion pumps have cyber flaws, putting them at risk from hackers: study

Published March 9, 2023

75% of infusion pumps used to deliver medication and fluids in hospitals have cyber flaws, putting them at risk from hackers, a new study by the UK's National Cyber Security Centre (NCSC) has revealed.

A study of over 100 infusion pumps from various medical device manufacturers, using open-source data and publicly available information, found that 75% of the devices were vulnerable to "critical" and "high" severity cyberattacks. The study also found that 40% of the devices had the potential to put lives at risk or require sensitive patient data to be accessed to use the device properly.

The study also found that 40% of the devices were vulnerable to "critical" and "high" severity cyberattacks. The study also found that 40% of the devices had the potential to put lives at risk or require sensitive patient data to be accessed to use the device properly.

digitalhealth

Client data exfiltrated in Advanced NHS cyber attack

Advanced NHS Cyber Security Unit (ACSU) has confirmed that the exfiltration of client data in the Advanced NHS cyber attack was successful.

The exfiltration of client data was confirmed by the ACSU, which is the lead agency for NHS cyber security. The exfiltration of client data was confirmed by the ACSU, which is the lead agency for NHS cyber security.

digitalhealth

Client data exfiltrated in Advanced NHS cyber attack

Advanced NHS Cyber Security Unit (ACSU) has confirmed that the exfiltration of client data in the Advanced NHS cyber attack was successful.

The exfiltration of client data was confirmed by the ACSU, which is the lead agency for NHS cyber security. The exfiltration of client data was confirmed by the ACSU, which is the lead agency for NHS cyber security.




HEIR
a secure Healthcare
Environment for Informatics
Resilience

Terminology

Vulnerability
Threat
Attack

07/03/2023 Introduction to Cybersecurity H2020 Grant Agreement 883275 – HEIR 6




HEIR
a secure Healthcare
Environment for Informatics
Resilience

Why attacks ?

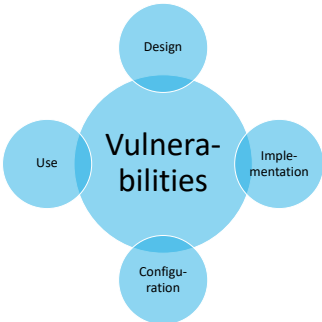
- Networks and information systems are a major contributor to economic value.
 - Monetary value
 - Information
 - Support for essential services
- There are still young with few constraints
 - Recent regulations
 - General Data Protection Regulation
 - Network and Information Security (NIS) directives
 - e-Privacy, e-Eidas, ...
 - Technologies and uses developing faster than secure and safe practices
- Thus they are a privileged target
 - Easy to create significant perturbations
 - Attribution very difficult
 - Consequences almost inexistant
 - Geopolitical strategic advantage

07/03/2023 Introduction to Cybersecurity H2020 Grant Agreement 883275 – HEIR 7



HEIR
a secure Healthcare
Environment for Informatics
Resilience

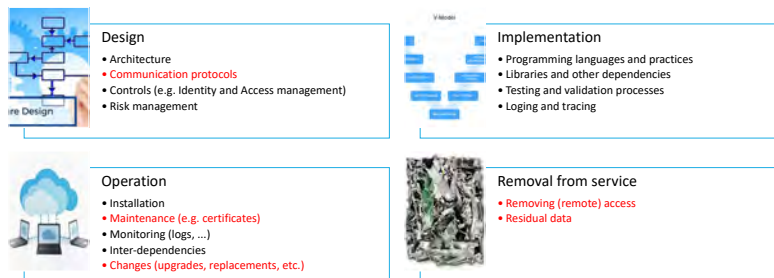
Vulnerability: **weakness** of an element of the IT system or network



- Many possible causes
 - Design
 - Wireless Equivalent Privacy (WEP)
 - Implementation
 - Wrong coding practices: buffer overflows, SQL injection
 - Configuration and operation
 - Weak passwords
 - Use
 - Spam and phishing
- Hardware as well as software
 - Spectre, Meltdown, ...

07/03/2023 Introduction to Cybersecurity H2020 Grant Agreement 883275 – HEIR 8

Vulnerabilities origin during the IT lifecycle



07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

9

Threat



- Potential **cause** of an incident
- Using one or several **vulnerabilities**
- Having an **impact** on the system
- That could cause damages if this threat is realized



07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

10

Attack



- **Malicious** action aimed at compromising a system
 - An attack represents a concrete threat using a (set of) vulnerabilities
- Benefit for the attacker: resources (data, ...), money, information
- Impact for the victim
 - Increased operational expenses
 - Reduced income
 - Theft
- 2 categories of attackers
 - Carpet-bombing
 - Targetted attacks

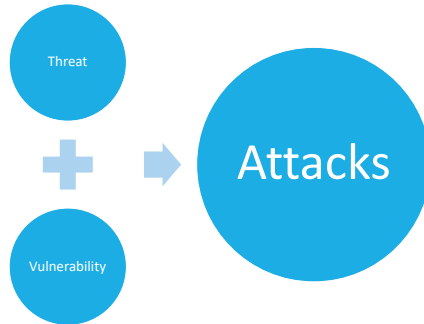
07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

11

In a nutshell



07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

12

Malicious code a.k.a. « Malware » (Ransomware, ...)



Computer viruses (malware) are « *massive attacks* »

- They tend to focus on specific targets
- They become increasingly hard to detect
- Nation states are devoting significant effort to these new weapons



Recent malware: Citadel, Flame, Stuxnet, Duqu, Conficker, Zeus, Shamoon (Aramco)...

- Main infection vectors
- Email with attachment
 - Removable device (USB key)
 - Malicious website
 - Open network shares
 - ...

- Potential impact...
- Trojan horse for remote access
 - Exfiltration of sensitive data
 - Remote surveillance
 - Ransomware
 - Data destruction
 - ...

2022/01/07

Cybersecurity - Hervé Debar

H2020 Grant Agreement 883275 – HEIR

13

HEIR Threat Hunting

(video)



07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

14

HEIR Privacy-Aware Framework

(video)

07/03/2023 Introduction to Cybersecurity H2020 Grant Agreement 883275 – HEIR 15

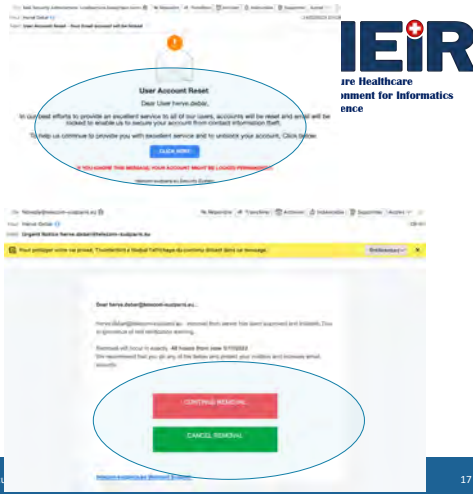
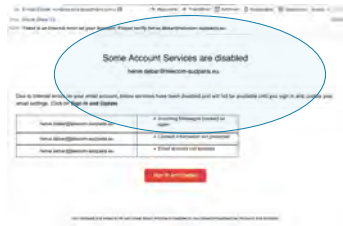
Practical cyber-hygiène

07/03/2023 Introduction to Cybersecurity H2020 Grant Agreement 883275 – HEIR 16

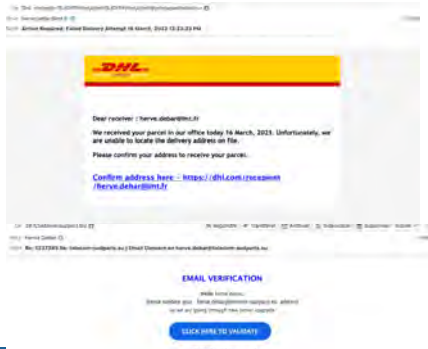
Problematic topic

07/03/2023 Introduction to Cybersecurity H2020 Grant Agreement 883275 – HEIR 17

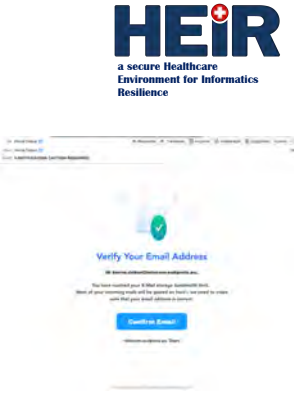
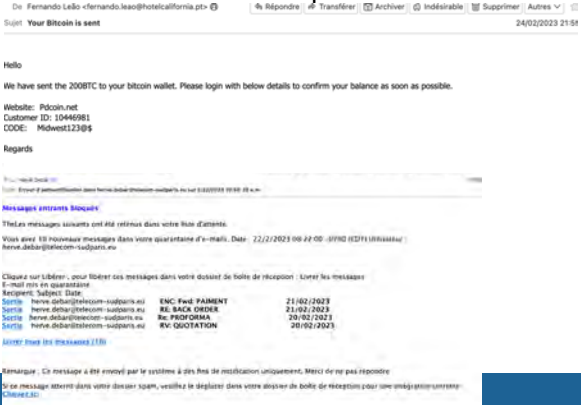
Problematic topic



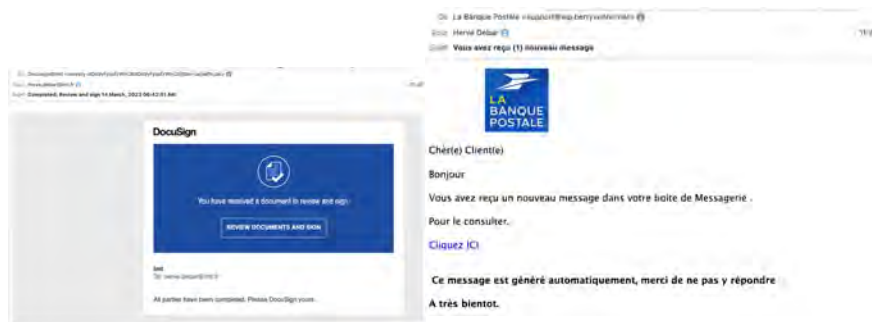
Strange links and requests



Unsolicited requests



Banks ...



07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

21

Beware of information overload



- Continuous stream of emails
- Regular practice shifts of attackers
 - Emails
 - Attachements
 - Calendar invites
- Next ?

07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

22

Maintain devices



- Tablets, smartphones, laptops, ...
- Software updates
 - Operating system
 - Applications
- Connectivity
 - Open wifi networks

07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

23

Authentication



- Ensure authenticated access to services
 - Single-sign-on
- Ensure web server name authentication
 - Systematic HTTPS

07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

24

Passwords



- Key security element
- Some are more sensitive than others
 - One or two key email accounts
- Password management
 - Local application
 - Web-based
 - Browser-based
- Prefer two-factor authentication
- Recovery
 - Recovery codes
- Hardware tokens

07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

25

Accept security mechanisms



- Network filtering
- Access control
 - Avoid shared passwords
 - Leverage single-sign-on
- Email filtering

07/03/2023

Introduction to Cybersecurity

H2020 Grant Agreement 883275 – HEIR

26