D7.9

Final Business Model and Long-Term Sustainability Report

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

Deliverable type	Report
Deliverable reference no.	D7.9
Workpackage	WP7
Due date	08-2023 –M36
Actual submission date	30/08/2023

Deliverable lead	Sphynx Technology Solutions AG (STS)
Editors	STS
Contributors	STS, IMT, FORTH, TUD, AEGIS, STELAR, SIE, FORTH, IBM, ITML, BD
Reviewers	FORTH, IMT
Dissemination level	PU
Revision	1.0
Keywords	Exploitation, Business Plan, Sustainability

Abstract

This deliverable presents the final business model and marketing approach for the overall HEIR outcome, which comprises several advanced components addressing a large set of real security needs in the healthcare domain. This deliverable also presents how HEIR collaborated with the Horizon Results Booster team to enhance its final strategy.

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

Executive Summary

This deliverable is a crucial component of the work conducted in WP7, encompassing the final HEIR market analysis and business plan. The plan outlines a comprehensive suite of advanced tools, as well as individual components available as standalone solutions, catering to the security needs of the rapidly expanding Healthcare, Machine Learning and Cybersecurity Markets.

The primary value proposition of HEIR stems from its extensive range of advanced offerings. Firstly, it provides real-time threat-hunting services, protecting healthcare organizations against the ever-increasing threat landscape. Secondly, HEIR enables improved and secure data-sharing, through its privacy-aware framework. This framework strongly emphasizes the trustworthiness of sensitive data and facilitates secure and confidential sharing of such data. It ensures that privacy and data protection standards are effectively upheld, providing stakeholders with confidence in handling sensitive information. Lastly, HEIR provides the Observatory for the Security of Electronic Medical Devices. This observatory serves as an intelligent knowledge base accessible to a wide range of stakeholders.

The business model of HEIR revolves around providing a marketplace for security components and privacy-aware solutions. The HEIR marketplace[1] encompasses a detailed description of the overall HEIR platform, highlighting the security needs addressed and the unique characteristics and advantages it offers. Additionally, it provides individual descriptions of all the components, outlining the security requirements each component addresses, along with their novel features and advantages.

Potential customers will have the flexibility to request the entire HEIR platform comprising all components, a specific set of components, or a single component as needed. The main point of contact will assist customers in finding descriptions of scenarios where several components have successfully worked together to achieve significant results. They will direct customers to the appropriate department of the HEIR partners who possess, exploit, and/or market the required components.

Moreover, each partner has selected their specific exploitation strategies for their components, such as offering them as a service, with one-off purchase fees, or providing them for free with paid support. This integrated marketing strategy for all components aims to benefit all partners, as potential customers seeking even a single component will be exposed to all the novel HEIR subsystems. Consequently, customers may consider additional components if further security needs arise, providing a win-win situation for both HEIR and its clients.

[1] https://heir2020.eu/marketplace/

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Scope and Objectives of the Deliverable

The primary goal of the HEIR project is to develop, validate, demonstrate, and support a holistic cyber-intelligence platform for secure healthcare environments. This framework enables secure data exchange across healthcare and research organisations, while ensuring a high degree of resilience, reliability, accountability, and trustworthiness. Additionally, it addresses threat prevention, detection, mitigation, and real-time response. Given the significant contributions of HEIR to the healthcare domain, a crucial aspect of the project is to identify the corresponding market needs.

This deliverable presents the final business plan of the HEIR project, with the main objective of driving the exploitation of project results after its conclusion. Specifically, the deliverable focuses on achieving Milestone #6 as it emphasizes the importance of ensuring business continuity and long-term sustainability during and after the project's lifetime.

Furthermore, the deliverable addresses the relevant Key Performance Indicators (KPIs) associated with MS#6 and Task 7.6. It delves into the analysis of non-technical aspects of cybersecurity and digital privacy, such as business viability and business alliances and collaborations. The report represents the outcome of continuous market analysis and the development of plans for the exploitation of both tangible and intangible assets generated by the project.

1.2 Structure Of the Deliverable

In this deliverable, we first report the market analysis conducted for the cybersecurity domain focusing on the key enabling technologies offered by HEIR, such as real-time threat monitoring, machine learning and blockchain techniques, as well as cybersecurity tools.

Next, we report HEIR’s value proposition and main exploitable assets, as well as the final HEIR Business Model and marketing strategy.

This deliverable also includes HEIR’s Marketplace and the final market analysis of the Healthcare and Cyber Security markets. It provides comprehensive insights into the size and growth forecasts, segmentation, and analysis of stakeholders within these markets.

Based on the outcomes of these analyses, the competitive advantage of HEIR has been identified through both a PEST analysis (Political, Economic, Social, and Technological factors) and a SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats). These analyses serve to highlight the unique strengths and opportunities of HEIR, as well as address potential challenges and threats in the market landscape. Overall, this section provides a comprehensive assessment of the market environment and the positioning of HEIR within it.

The deliverable concludes with a description of HEIR’s approach to Intellectual Property protection.

2. Market Analysis For Cybersecurity in the Healthcare Domain

With the implementation of electronic health records, telemedicine, and connected medical equipment in recent years, the healthcare sector has undergone tremendous digital change. While these developments have increased operational effectiveness and patient care, they have also exposed the healthcare industry to previously unheard-of cybersecurity vulnerabilities. This market research examines the main trends, problems, and growth prospects in this industry as it pertains to cybersecurity in the healthcare industry today.

The rising frequency and sophistication of cyberattacks against healthcare-related organizations (hospitals, public administrations, companies, etc.) is one of the key trends in the market for healthcare cybersecurity. Patient data theft, ransomware attacks, and outages of vital healthcare systems are now frequent occurrences. As a result, healthcare organizations are making significant investments in cybersecurity solutions to safeguard their systems, networks, and patient data from nefarious individuals.

The regulatory environment also has a significant impact on how the healthcare cybersecurity market is shaped. The urgent need to address cybersecurity in healthcare has been acknowledged by governments and regulatory authorities around the world. As a result, they have put into place strict data privacy rules and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Privacy Regulation (GDPR) in Europe. Healthcare firms now place a high focus on complying with these requirements, which is fueling the demand for reliable cybersecurity solutions.

These factors collectively imply that the healthcare industry presents substantial growth potential for suppliers of cybersecurity solutions. There is a significant need for cybersecurity services in the healthcare industry due to the rising awareness of cyber dangers and the growing reliance on digital technologies. Protecting sensitive patient data and preserving the integrity of healthcare systems requires solutions including network security, data encryption, threat intelligence, and employee training.

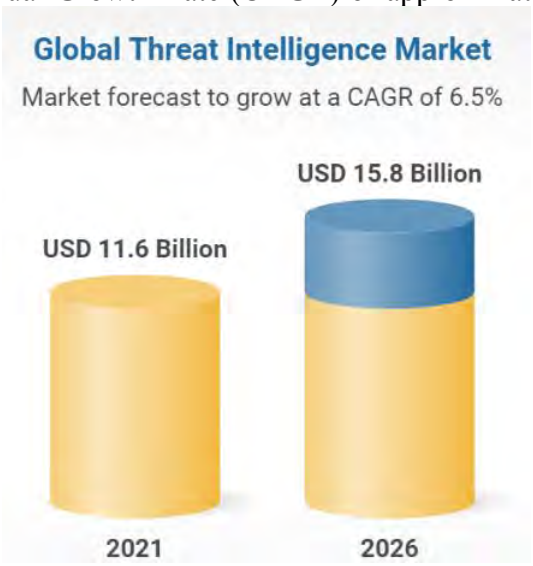
Taking all these aspects into account means that cybersecurity solutions developed specifically for the unique requirements and difficulties faced by the healthcare industry have a big potential to significantly improve the security and resilience of healthcare organizations. Healthcare providers can efficiently reduce risks, protect patient data, and guarantee continuous access to essential healthcare services by putting strong cybersecurity safeguards in place. These tailored solutions address compliance standards, privacy issues, and the intricate web of interconnected healthcare systems in addition to providing advanced threat detection and prevention capabilities. The healthcare sector can confidently embrace digital advances and provide high-quality care while upholding the trust and confidence of patients and stakeholders with the proper cybersecurity protections in place.

2.1 Key Enabling Technologies

2.1.1 Real-time Threat Monitoring Market Analysis

Real-time threat monitoring refers to the continuous monitoring of digital systems and networks to identify and respond to potential threats in a real-time manner (Victor R. Kebande, 2021). With the increasing frequency and sophistication of cyber-attacks, organizations across various sectors are investing in real-time threat monitoring solutions to safeguard their critical assets, protect sensitive data, and ensure business continuity. This market analysis aims to provide an overview of the real-time threat monitoring market, including key trends, growth drivers, major players, and future prospects.

The real-time threat monitoring market has experienced substantial growth in recent years and is expected to continue expanding at a significant rate[2]. The growing awareness of cybersecurity risks, stringent regulatory requirements, and the increasing adoption of cloud-based technologies are some of the primary factors contributing to the market's growth. According to market research reports, the global threat intelligence market was valued at USD 11.6 billion in 2021 and is projected to reach USD 15.8 billion by 2026, growing at a Compound Annual Growth Rate (CAGR) of approximately 6.5% during the forecast period[3], as illustrated in Figure 1.



Global Threat Intelligence Market
Market forecast to grow at a CAGR of 6.5%
USD 15.8 Billion
USD 11.6 Billion
2021
2026

Figure 1 Global Threat Intelligence Market Forecast 2021-2026[4]

[2] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[3] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
[4] https://www.researchandmarkets.com/reports/5230051/global-threat-intelligence-market-with-covid-19?utm_source=GNOM&utm_medium=PressRelease&utm_code=txpgkp&utm_campaign=1677789+-+Global+Threat+Intelligence+Markets+Report+2022-2026+-+Increasing+Instances+of+Phishing+Attacks+and+Spams+to+Drive+the+Demand+for+Threat+Intelligence+Solutions&utm_exec=chdo54prd

Because of the growing need for effective and efficient tools to deal with the increasing number and frequency of cyber-attacks, various key trends have formed in the market over the past few years. Specifically, the increasing sophistication of cyber-attacks led organizations to increasingly seek comprehensive threat detection and response capabilities to counter these sophisticated attacks effectively[5]. Additionally, the adoption of artificial intelligence and machine learning in real-time threat monitoring solutions has gained prominence, enabling the detection of anomalous behavior, identification of new threat patterns, and automation of response actions, enhancing the overall efficiency and effectiveness of threat monitoring (T. C. Truong, 2020). Furthermore, the rapid adoption of cloud computing and the proliferation of cloud services forced organizations to shift towards cloud-based threat monitoring solutions, offering scalability, flexibility, and ease of deployment, making them attractive for businesses of all sizes[6]. In parallel, the increasing regulatory compliance requirements, such as GDPR and CCPA, have compelled organizations to implement robust threat monitoring solutions to safeguard customer data and comply with legal requirements. This has further propelled the demand for real-time threat-monitoring solutions across various industries[7,8].

This market consists of several key players, that achieved a well-established instance over the years through the successful promotion of their cybersecurity-related products, and consequent high customer satisfaction and trustworthiness. A description of products and services of several top key players providing cybersecurity and real-time threat monitoring is shown in Table 1.

Table 1 Key players and products/services in the real-time threat monitoring market

Company	Product/Service	Main Feature
Splunk	Splunk Enterprise Security[9]	Real-time security monitoring, threat detection, log analysis, incident response automation, and correlation of data from various sources.
IBM	IBM QRadar[10]	Real-time threat detection and monitoring, SIEM, advanced analytics, behavioral anomaly detection, and integration with various security tools.
Cisco	Cisco Threat Grid[11]	Automated malware analysis, threat intelligence, real-time monitoring of file behavior, sandboxing, and integration with other security products.

[5] https://threatpost.com/cybercrime-more-sophisticated/179676/
[6] https://www.securonix.com/solutions/cloud-security-monitoring/
[7] https://www2.deloitte.com/cn/en/pages/operations/articles/soe-transformation-whitepaper-issue6.html
[8] https://healthaxis.com/healthcare-regulatory-compliance/
[9] https://www.splunk.com/en_us/products/enterprise-security.html
[10] https://www.ibm.com/qradar
[11] https://www.cisco.com/c/en/us/products/security/threat-grid/index.html

McAfee	McAfee MVISION[12]	Real-time threat intelligence, proactive detection of advanced threats, behavior-based analytics, cloud-based security, and integration with other security solutions.
Palo Alto Networks	Palo Alto Networks WildFire[13]	Advanced threat detection and prevention, sandboxing, analysis of unknown files, machine learning-based malware detection, and integration with Palo Alto's security platform.

The real-time threat monitoring market is experiencing robust growth due to the escalating cybersecurity threats and the need for proactive security measures. Organizations are recognizing the importance of continuous threat monitoring to protect their critical assets and ensure operational resilience. Factors such as the increasing frequency and complexity of cyber threats, the growing adoption of IoT devices, and the rise of advanced technologies like 5G and edge computing are anticipated to drive the market further[14]. Additionally, the emergence of new regulatory frameworks and the need for proactive threat detection and response capabilities will fuel the demand for real-time threat monitoring solutions across industries. As the market continues to evolve, the integration of advanced technologies and the development of comprehensive solutions will play a crucial role in addressing the dynamic nature of cyber threats and providing effective real-time threat monitoring capabilities.

2.1.2 Cybersecurity tools Market Analysis

Extended Detection and Response (XDR) is an integrated suite of security products that merge and improve detection capabilities and automated response to security incidents. It is an evolution of Endpoint Detection and Response (EDR) and encompasses more sources of data to increase detection accuracy.

Market Analysis:

1. Market Size: The XDR market is experiencing substantial growth due to the increasing frequency and complexity of cyber-attacks, which standard security protocols struggle to deal with. As cyber threats become more advanced and sophisticated, the demand for comprehensive solutions like XDR is likely to increase significantly.
2. Key Players: Major cybersecurity vendors such as Palo Alto Networks, Microsoft, Trend Micro, Symantec, and others have introduced their XDR offerings and are key players in the market.
3. Adoption Rate: Organizations across various sectors, including healthcare, financial services, and government, are adopting XDR solutions for enhanced security. The

[12] https://cybersecurity-excellence-awards.com/candidates/mcafee-mvision-endpoint-2/
[13] https://www.paloaltonetworks.com/network-security/wildfire
[14] https://www.fortunebusinessinsights.com/edge-computing-market-103760

rising trend of remote work and cloud-based services due to the COVID-19 pandemic is driving the uptake of XDR solutions.

4. Geographical Distribution: North America and Europe lead the way due to their higher adoption of advanced cybersecurity solutions. However, the Asia Pacific region is likely to witness the fastest growth due to increasing digital transformation and awareness about cybersecurity.

Forecast (2023-2028):

1. Growth Rate: The XDR market, valued at 0,75B in 2022 (Grand View Research, 2023) is expected to grow at a compound annual growth rate (CAGR) of 20.7% from 2023 to 2030. The increasing trend of digital transformation and the rising frequency of cyberattacks are key factors propelling this growth.
2. Technological Innovation: As the technology evolves, more advanced XDR solutions are expected to be developed, offering more comprehensive and efficient protection against cyber threats. The integration of artificial intelligence and machine learning in XDR could be a game-changer in the market.
3. Regulatory Influence: Increasing cybersecurity regulations and guidelines would force organisations to strengthen their security infrastructure, potentially leading to increased adoption of XDR solutions.
4. Competitive Landscape: The competitive landscape is likely to intensify, with more vendors entering the market and existing players innovating their offerings. Strategic partnerships, mergers, and acquisitions could be common as companies look to strengthen their market presence.
5. Potential Challenges: Despite its potential growth, the market could face challenges like high costs, complex integrations, and lack of skilled professionals in the field. Addressing these issues will be crucial for continued growth in the sector.

2.1.3 Machine Learning Market Analysis

The Machine Learning Market Analysis is a pivotal aspect of understanding the current landscape and trends in the field of machine learning. Over the past decade, machine learning has experienced exponential growth and transformative advancements, revolutionizing various industries and applications. Before the widespread adoption of machine learning, businesses heavily relied on traditional rule-based systems, which often needed to be improved in handling complex and unstructured data. However, with the advent of modern machine learning algorithms and the availability of vast amounts of data, the landscape has drastically changed.

Today, machine learning has become an indispensable tool for organizations across diverse domains. According to industry reports, the global machine-learning market was valued at $15.47 billion in 2021 and is projected to reach $305.62 billion by 2030, growing at a CAGR of 39.3% during the forecast period (See Figure 2). This staggering growth is a testament to the increasing recognition of machine learning's potential to drive innovation, improve operational efficiency, and create data-driven solutions[14]. Table 2 presents an overview of key players in the cybersecurity and real-time threat monitoring market. The table showcases their market size, growth rate, and covered segments, providing valuable insights into the industry's landscape and offerings.

During the Machine Learning Market Analysis, multiple algorithms are typically applied to diverse datasets to gauge their performance in solving specific tasks. For instance, classification models using algorithms such as Support Vector Machines (SVM) and Random Forests have shown significant improvements in accuracy and precision compared to traditional rule-based methods. Regression models, such as Gradient Boosting and Neural Networks, have demonstrated remarkable predictive capabilities, enabling businesses to make data-driven decisions and forecasts with unprecedented accuracy.

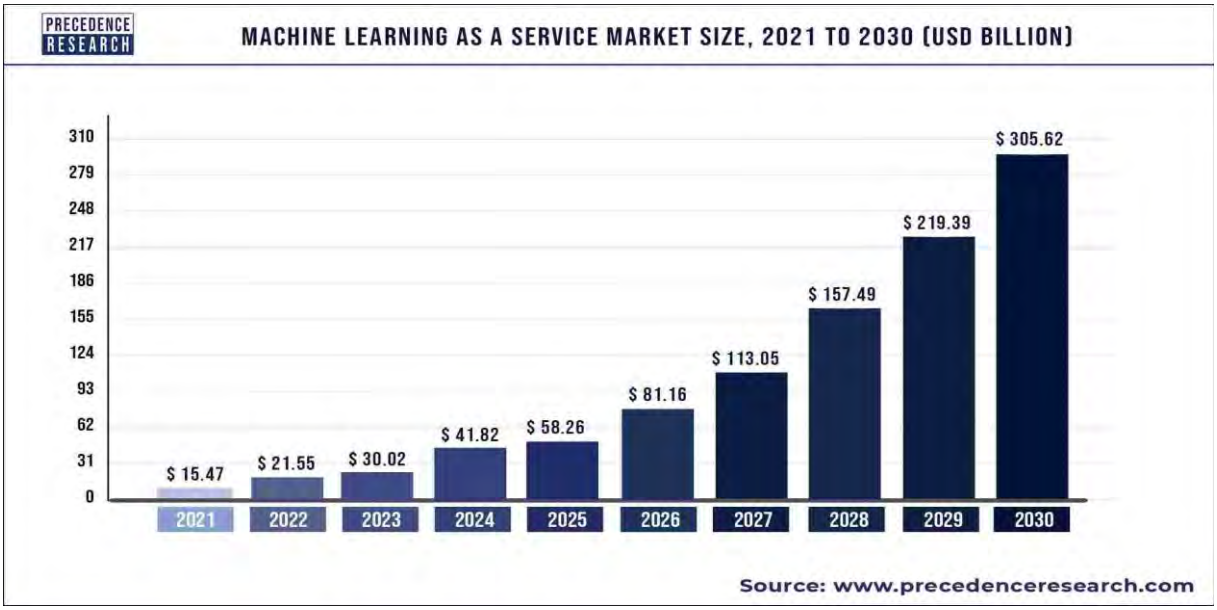


Figure 2 Machine Learning Market Value From 2021 to 2030

Moreover, the analysis explores the impact of hyperparameter tuning, feature engineering, and data preprocessing on the overall performance of the models. With advancements in automated hyperparameter optimization techniques and feature selection algorithms, machine learning practitioners can now achieve better model performance with reduced manual effort.

Table 2 Report Scope of the Machine Learning as a Service Market

Report Coverage	Details
Market Size in 2022	USD 21.55 Billion
Market Size by 2030	USD 305.62 Billion
Growth Rate from 2022 to 2030	CAGR of 39.3%
Base Year	2021
Forecast Period	2022 to 2030
Segments Covered	Component, Organization Size, Application, Industry Vertical, Geography
Companies Mentioned	GOOGLE INC, SAS INSTITUTE INC, FICO, HEWLETT PACKARD ENTERPRISE, YOTTAMINE ANALYTICS, AMAZON WEB SERVICES, BIGML, INC, MICROSOFT CORPORATION, PREDICTRON LABS LTD, IBM

	CORPORATION

2.1.4 Blockchain Market Analysis

This market analysis report provides an in-depth assessment of the market landscape, trends, challenges, and opportunities surrounding the blockchain-based applications in different industries and in healthcare more specifically. The analysis is based on the assessment of current trends in this domain and the assumptions in the technology evolution.

The blockchain market has experienced significant growth in recent years, and the growth is expected to continue over the next years. More specifically, the overall blockchain market size was estimated to $7.4 billion in 2022, and is projected to reach the $94.0 billion in 2027, growing at CAGR of 66.2% in this forecasted period.[15] The potential of this industry is also highlight on level investment on several blockchain application and ventures. These are usually focused on payment, exchanges, smart contracts, documentation and digital identities.

In healthcare, the blockchain-related market size is projected to reach $19.52 million in 2028, growing at CAGR of 52.48%.[16] This growth, is closely linked with the increase acceptance and use of blockchain-as-a-service (BaaS) applications. Such activities include solutions for tackling challenges related with supply chain management, smart contracts, the privacy of individual health information, technical problems with data management, the ability to use different payment models, and tracking virus outbreaks.

Focusing on the Hyperledger (the blockchain (Fabric Project) utilized in HEIR), it is a leading permissioned blockchain platform that offers immense potential for transforming industries. Its features, modularity, and industry collaborations position it as a key player in the blockchain market.[17] It has several applications in various domains, while in healthcare an increasing number of initiatives can be found, covering its entire supply chain (e.g., Axuall, KitChain, MELLODY project, MyClinic.com etc).[18]

In 2020, Hyperledger Fabric 2.0 was released in order to tackle some of the identified problems of high-complexity, resilience, scalability and the and network delays. Despite the fact that this update was not revolutionary in terms of simplicity or applicability, it demonstrated that progress on the evolution of this technology in on the move and independent from the developments in the cryptocurrency domain.[19] This is considered very important, as it proves that enterprise blockchain will undoubtedly find its proper use. Therefore, and by taking into account the aforementioned market trends, with the increasing adoption and ongoing advancements, Hyperledger Fabric is expected to shape the future of decentralized systems and contribute to the broader adoption of blockchain technology.

[15] https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html [Last visited on: 19/07/2023]
[16] https://www.mordorintelligence.com/industry-reports/blockchain-market-in-healthcare [Last visited on: 19/07/2023]
[17] https://www.hyperledger.org/learn/publications/hyperledger-annual-report-2020 [Last visited on: 19/07/2023]
[18] https://www.hyperledger.org/blog/2020/01/29/five-healthcare-projects-powered-by-hyperledger-you-may-not-know-about [Last visited on: 19/07/2023]
[19] https://www.investopedia.com/terms/h/hyperledger-fabric.asp [Last visited on: 19/07/2023]

2.1.5 Commodity Cluster of GPUs Market Analysis

The commodity cluster of GPUs has emerged as a significant segment within the rapidly evolving computer hardware industry. Originally designed to handle graphics-intensive tasks, GPUs have grown to become crucial components in parallel processing and artificial intelligence applications. Commodity clusters of GPUs refer to grouping multiple GPUs into a unified system, offering unparalleled computational power and efficiency.

The market of GPU clusters has witnessed remarkable growth over the past few years, driven by the increasing demand for high-performance computing in various industries. Applications in scientific research, artificial intelligence, machine learning, data analytics, and gaming have propelled the market forward. The ability of GPU clusters to handle massively parallel processing tasks has revolutionized industries by accelerating complex computations and enhancing overall performance.

Some of the key market drivers are the following:

- ***Rise of Artificial Intelligence and Machine Learning:*** The proliferation of AI and ML applications in diverse sectors like healthcare, finance, automotive, and e-commerce has fueled the demand for GPU clusters. GPUs' capability to handle large-scale parallel processing tasks makes them ideal for training and inference processes.
- ***Data Explosion:*** The exponential growth of data generated from various sources necessitates more advanced and efficient processing capabilities. Commodity GPU clusters offer cost-effective solutions for processing and analyzing vast amounts of data in real-time.
- ***High-Performance Computing (HPC) Applications:*** Sectors like scientific research, weather forecasting, and simulations heavily rely on powerful computing systems. GPU clusters provide the required computational power for these resource-intensive tasks.

At the same time, GPU clusters face significant market challenges:

- ***Cost Constraints:*** While commodity GPU clusters are more affordable than specialized supercomputers, their costs can still be prohibitive for smaller businesses and research institutions, limiting their adoption.
- ***Power Consumption:*** High-performance GPU clusters consume significant power, leading to increased operating costs and concerns over environmental impact.
- ***Cooling and Infrastructure:*** Cooling requirements for GPU clusters can be substantial, requiring robust infrastructure and cooling solutions to prevent overheating and maintain performance.
- ***Market Consolidation:*** The market is dominated by a few major players, potentially limiting competition and innovation, leading to higher prices and restricted access to cutting-edge technologies.

Overall, the GPU clusters' market is poised for significant growth, driven by the increasing demand for high-performance computing, AI, and data-intensive applications. Despite cost and power consumption challenges, the market's potential remains promising, particularly with the advent of edge computing and cloud-based services. To harness the full potential of GPU clusters, industry players must focus on innovation, cost optimization, and accessibility to ensure a sustainable and thriving market ecosystem. As technology advances, the GPU clusters' market is set to play a pivotal role in shaping the future of computing across industries.

2.1.6 Visualizations Market Analysis

The global healthcare analytics market was valued at $35.3 billion in 2022. Growing at a CAGR of 21.4%, it is projected to reach $167.0 by 2023[20]. The European Healthcare data visualization market size was worth USD 4.28 billion in 2023 and is estimated to be a market of USD 13.9 billion by 2028 with a growth rate of 26.52% during the forecast period[21]. The data visualization market, segmented by component, comprises two key components: software and services. Regarding a breakup by deployment mode, the market comprises two modes: cloud-based and on-premises. Geographically, the major regional markets for data visualization are North America, Europe, Asia Pacific, Latin America, and the Middle East and Africa. North America is the largest market for healthcare analytics, with the United States being the largest contributor to this market. The global healthcare analytics market is a part of the healthcare industry that is growing quickly. Healthcare analytics is the use of tools and techniques for data analysis to improve health outcomes, lower costs, and improve clinical and operational performance. This includes using "big data," "machine learning," and "artificial intelligence" to look at a lot of data about patients, like clinical, financial, and operational data.

The increasing adoption of visualization platforms for software advisory and predictive analysis is one of the key factors driving the growth of the market. Moreover, the increasing organizational demand for interactive and simplified projection of data is providing a thrust to market growth. Medium and large-scale enterprises are extensively utilizing data visualization systems through smartphones, desktops, tablets and web-based applications for generating customized reports and graphical representations of the data. In line with this, the increasing requirement for interactive dashboards based on unstructured data obtained from social media platforms, email service providers and smart devices is also contributing to the growth of the market. Additionally, various technological advancements, such as the integration of connected devices with artificial intelligence (AI), cloud computing and virtual reality (VR) solutions, are acting as other growth-inducing factors. Organizations use these technologies for cost-effective and scalable data analysis and identifying key performance indicators (KPIs) through business intelligence (BI). Other factors, including the increasing adoption of data visualization tools in the retail industry, along with significant improvements in the IT infrastructure across the globe, are anticipated to drive the market toward growth.

The data visualization market on a global scale is characterized by strong competition, with both established players and emerging startups battling for market share. The profiles of the key players are Alteryx Inc., Domo Inc., Dundas Data Visualization Inc., Hitachi Ltd., InetSoft Technology Corp., International Business Machines Corporation, Microsoft Corporation, MicroStrategy Incorporated, Oracle Corporation, Salesforce.com Inc., SAP SE, SAS Institute Inc. and TIBCO Software Inc[22].

Regarding the software, key competitors include:

- Tableau Software: A renowned leader in data visualization, it is a data visualization and analytics platform that enables users to explore data and share insights. Users can build

[20] https://www.globenewswire.com/en/news-release/2023/04/07/2643067/0/en/Healthcare-Analytics-Market-Is-Expected-to-Reach-USD-167-0-Billion-by-2030-Grow-at-a-CAGR-Of-21-4-during-Forecast-Period-2023-To-2030-Data-By-Contrive-Datum-Insights-Pvt-Ltd.html

[21] https://www.marketdataforecast.com/market-reports/europe-healthcare-analytics-market

[22] https://www.imarcgroup.com/data-visualization-market

visualizations with drag and drop, employ Artificial Intelligence-driven statistical modelling with a few clicks and ask questions using natural language.

- Microsoft Power BI: A business intelligence platform that enables users to collaborate with data and track goals. It provides real-time analytics and trend analysis to help users make confident decisions. Microsoft Power BI integrates with many Microsoft products and cloud services, making it a versatile solution for businesses. In addition, it offers data security features to protect user data.
- Qlik Sense: It is a data visualization tool that uses artificial intelligence (AI) to help users understand and use data more effectively. It offers deeper interactivity and broad context, as well as lightning-fast calculations and the ability to connect and combine data from hundreds of data sources. Qlik Sense is a part of the Qlik Active Intelligence Platform, which offers analytics performance and scalability to businesses of all sizes. Additionally, it's available as a software-as-a-service (SaaS) solution or as a hybrid service that extends SaaS analytics to on-premises data.
- Klipfolio: It grants access and combines data from hundreds of services without writing any code using curated instant metrics, all of which are pre-built. With its powerful data modeller, you can leverage data in everyday decision-making. Users can import, edit and analyze data to get comprehensive and exact insight.
- Looker: It is a tool that allows users to see data in many ways thanks to its plugin marketplace. Different types of visualizations, such as bar gauges, aster plots, cartoons, calendar heat maps, liquid fill gauges and spider visualization are available. It has pre-made analytical blocks that let users employ templates for certain data or analyses, which helps to accelerate analytics.
- Zoho Analytics: It is a data visualization tool that allows users to import data from a variety of data sources for in-depth analysis. With a drag-and-drop interface, users can create insightful reports and dashboards with a range of data visualization tools. Also, users can collaborate on reports and dashboards with their coworkers and decide what others may see and do with the reports provided to them.
- Domo: It provides data visualization tools that help small businesses understand data and make data-driven decisions. With its easy-to-use interface, it allows users to create custom apps, advanced charts and maps and other visualizations of data with just a few clicks. Its governance tools help organizations control who has access to data.

In the healthcare sector, the data visualization market presents significant growth potential. Currently, there are limited players specifically targeting this segment. Key competitors in this specialized domain include[23]:

- IBM Watson Health: A prominent player offering healthcare analytics and visualization solutions, with a specific focus on medical data analysis and insights.
- Optum Data Visualization Services: includes a customizable dashboard that draws from unique data sets built from your existing data sources and repositories, such as data warehouses, APCDs, MMIS systems, eligibility systems, and others.
- SAS Institute: Provides healthcare analytics tools that enable data exploration, visualization, and predictive modeling for healthcare organizations.
- Health Catalyst: Offers a suite of healthcare analytics solutions, including applications for data visualization and performance improvement.

These competitors in the healthcare segment are a sample of the growing demand for advanced visualization tools tailored specifically for the unique challenges and requirements of the healthcare industry.

[23] https://www.marketdataforecast.com/market-reports/europe-healthcare-analytics-market

2.1.7 Digital Forensics Market Analysis

The global digital forensics market attained a value of USD 8.35 billion in 2021, driven by the increased prevalence of cybercrimes worldwide. Aided by heightened technological advancements, the market is expected to witness further growth in the forecast period of 2023-2028, growing at a CAGR of 15.95%. The market is projected to reach USD 20.29 billion by 2027[24]. The rise in the number of cyber-attacks, malware, ransomware, and other malpractices to acquire data through illicit means has increased investments in digital forensics solutions. Moreover, the rise in government regulations to comply with data protection norms has also increased the demand for the Digital Forensics Market[25].

The digital forensics market comprises three key components: hardware, software, and services. Geographically, the major regional markets for digital forensics are North America, Europe, Asia Pacific, Latin America, and the Middle East and Africa. Notably, the healthcare sector encounters unique challenges in forensic investigations, particularly related to medical malpractice, insurance fraud, and patient safety. Traditional methods of analyzing medical and forensic data often involve manual review and interpretation, leading to time-consuming processes and a higher risk of errors. To address these challenges, a specialized forensics visualization tool tailored specifically for the healthcare sector has the potential to enhance investigation efficiency, accuracy, and decision-making.

Based on a recent report produced by Market Data Forecast, the European Healthcare Cybersecurity Market size was worth USD 3.22 billion in 2022 and is estimated to grow at a CAGR of 17,2% from 2022 to 2027. The largest market for healthcare cybersecurity is in North America, with Europe being in 2nd place.[26] The rise in the adoption of digital healthcare is increasing the demand for healthcare cybersecurity. At the same time, the rise in the number of cyberattacks in hospitals and medical clinics is fueling the demand for the healthcare cybersecurity market in Europe.

The forensics visualization market on a global scale is characterized by strong competition, with both established players and emerging startups battling for market share. Key competitors include:

- Palantir Technologies: Known for its advanced data analysis and visualization platform, Palantir provides solutions across various industries, including law enforcement and cybersecurity.
- ProDiscover Forensic: A comprehensive digital forensics software that empowers investigators to capture critical evidence from computer systems. It offers capabilities to handle all aspects of an in-depth forensic investigation, including evidence collection, preservation, filtering, and analysis.
- CAINE (Computer Aided INvestigative Environment): An Ubuntu-based application that provides a complete forensic environment with a user-friendly graphical interface. It can be seamlessly integrated into existing software tools as a module and automatically extracts a timeline from RAM.
- Magnet Forensics: Specializing in digital forensics software, Magnet Forensics offers a range of tools for data extraction, analysis, and visualization.
- Wireshark: A network packet analysis tool widely used for network testing and troubleshooting. It assists in examining different types of traffic flowing through computer systems.

[24] https://www.expertmarketresearch.com/reports/digital-forensics-market
[25] https://www.verifiedmarketresearch.com/product/digital-forensics-market/
[26] https://www.marketdataforecast.com/market-reports/european-healthcare-cybersecurity-market

In addition, SIEM, or Security Information and Event Management collects logs and events, normalizing this data for further analysis that can manifest as visualizations, alerts, searches, reports, and more. Security teams will often use their SIEM as a central dashboard, conducting many of their day-to-day operations out of the platform. Security analysts can use SIEM solutions to take on advanced cybersecurity use cases such as continuous monitoring, threat hunting, and incident investigation and response[27]. As a result, SIEM platforms may be considered competitors to the FVT. Key competitors include:

- Exabeam Fusion SIEM: Previously known as SaaS Cloud, is available as a SaaS in hybrid and local co-deployment. The solution includes components such as Advanced Analytics, Exabeam Data Lake, Threat Hunter, Case Manager, Incident Responder, Entity Analytics, Exabeam Cloud Connector, and Cloud Archive. These capabilities can be acquired separately to enhance existing SIEM products or bundled.
- IBM: Offers QRadar SIEM solutions as well as other security options such as Guardium, X-Force Threat Intelligence, Trusteer, Cloud Pak for Security, Privileged Identity Manager, Access Verification, WinCollect, QRadar Vulnerability Manager, and QRadar Network Insights.
- LogRhythm: Provides a SIEM platform that includes behavior analysis for endpoints, networks, and users. The solution offers cloud-hosted deployment. However, the majority of customers deploy this platform locally.
- Rapid7: Offers InsightIDR that runs on a cloud-based Insight platform. It provides additional products, including InsightVM (which offers vulnerability management), InsightConnect (which provides SOAR technology), InsightAppSec, Enhanced Network Traffic Analytics, and DivvyCloud (which offers Cloud Security Posture Management).
- Securonix: Offers next-generation SIEM, UEBA, security data lakes, SOAR, threat intelligence, NDR, and adversarial behaviour analysis. It also offers use-case-specific features, such as protection for SAP and healthcare environments.
- Splunk: Splunk SIEM provides products like Splunk Enterprise, Enterprise Security, Splunk Cloud, and Mission Control. High-quality SOAR and UEBA capabilities are also available but cannot integrate locally with other products. You can deploy Splunk products as software or through Splunk Cloud.

In the healthcare sector, the forensics visualization market is relatively niche but presents significant growth potential. Currently, there are limited players specifically targeting this segment. Key competitors in this specialized domain include:

- IBM Watson Health: A prominent player offering healthcare analytics and visualization solutions, with a specific focus on medical data analysis and insights.
- SAS Institute: Provides healthcare analytics tools that enable data exploration, visualization, and predictive modelling for healthcare organizations.
- Health Catalyst: Offers a suite of healthcare analytics solutions, including applications for data visualization and performance improvement.

These competitors in the healthcare segment are poised to tap into the growing demand for advanced forensics visualization tools tailored specifically for the unique challenges and requirements of the healthcare industry.

[27] https://www.elastic.co/what-is/siem

3. HEIR Value Proposition and Main Exploitable Assets

3.1 HEIR Business Model and Marketing Strategy

The business model of the HEIR project revolves around creating a marketplace for security component solutions. The marketplace (see Section 4) will feature a comprehensive description of the overall HEIR platform, highlighting the security needs addressed and unique characteristics and advantages. Additionally, detailed descriptions of each individual component will be provided, outlining the security requirements they address and their innovative features.

Each component will include (a) the problem that it tries to solve, (b) the proposed solution, and (c) its unique value proposition. This will allow external users and potential customers to identify the offerings of HEIR. Partners have also selected precise exploitation strategies for their components, such as providing them as a service, with one-off purchase fees, for free with paid support, etc.

In the subsequent sections, detailed descriptions of the different HEIR offerings will be provided in a marketable manner for inclusion in the HEIR marketplace. For both the overall platform and each component, the Business Model Canvas will be presented. This analysis includes various elements such as customer problems the product solves, target customer segments, unique value proposition, solutions matching customer problems, communication channels, expected revenue streams, cost structure, key metrics, and unfair advantage over competitors.

The Business Model Canvas approach has been adopted based on the advice of the Horizon Booster[28] service of the EC to enhance the efficiency of our business plans. We consulted with them to develop robust exploitation plans for the project. Even after the project's conclusion, several partners, including the partner responsible for HEIR's exploitation tasks, will continue to work with Horizon Booster to further enhance the exploitation potential of the project's novel results.

3.2 Marketing Description of the HEIR Offerings

3.2.1 The HEIR Platform

In the landscape of healthcare, significant challenges emerge in the realm of cybersecurity. The healthcare sector is increasingly becoming a prime target for cyber-attacks, necessitating heightened defensive measures. Unfortunately, there is a notable absence of comprehensive risk assessment mechanisms tailored to the healthcare domain, leaving critical vulnerabilities unaddressed. An additional concern arises from the limited availability of effective anomaly detection mechanisms, leaving healthcare systems prone to undetected breaches. Trustworthiness of healthcare-related data remains a hurdle, as robust mechanisms to ensure data integrity and authenticity are lacking. Furthermore, the scarcity of benchmarks for comparable healthcare organizations hinders the establishment of best practices and standards. Lastly, a noteworthy gap exists in the form of an intelligent knowledge base accessible to diverse stakeholders, inhibiting collaborative efforts to combat evolving threats effectively. The HEIR platform is a holistic cyber-intelligence platform for a secure healthcare environment that provides real-time threat-hunting capabilities, facilitated by advanced machine learning technologies, leads to the creation of the Risk Assessment for Medical

[28] https://www.horizonresultsbooster.eu/

Applications (RAMA) score in a local and global environment. Moreover, HEIR offers the Privacy-Aware Framework that enables sensitive data trustworthiness sharing by leveraging blockchain capabilities. Lastly, HEIR offers an intelligent knowledge base accessible to different stakeholders, providing advanced visualizations for each threat identified in RAMA and facilitating global awareness of EMD-related threats.

HEIR's Platform Business Model Canvas is available in Figure 3.

BUSINESS MODEL CANVAS

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITION	CUSTOMER RELATIONSHIP	CUSTOMER SEGMENTS
• Healthcare organizations and providers • Cybersecurity experts and consultants • Machine learning and AI technology providers • Blockchain technology providers • Data visualization and analytics companies	• Developing and maintaining the cyber-intelligence platform • Implementing advanced machine learning algorithms for threat detection • Creating and updating the Risk Assessment for Medical Applications (RAMA) score • Building and managing the Privacy-Aware Framework using blockchain technology • Curating and updating the intelligent knowledge base • Developing advanced visualizations for threat identification and awareness	• Real-time threat-hunting capabilities for a secure healthcare environment • Creation of the Risk Assessment for Medical Applications (RAMA) score • Privacy-Aware Framework for secure and trustworthy data sharing • Intelligent knowledge base with advanced threat visualizations • Global awareness of Emerging Medical Device (EMD)-related threats	• Healthcare institutions and hospitals • Medical device manufacturers • Cybersecurity professionals and consultants in healthcare • Regulatory authorities and compliance bodies	• Healthcare institutions and hospitals • Medical device manufacturers • Cybersecurity professionals and consultants in healthcare • Regulatory authorities and compliance bodies
	KEY RESOURCES • Advanced machine learning algorithms and models • Cybersecurity experts and data scientists • Blockchain technology infrastructure • Medical and cybersecurity data sources • Software development and IT infrastructure		**CHANNELS** • Online platform and web portal for accessing the HEIR services • Direct sales and partnerships with healthcare organizations • Participation in healthcare and cybersecurity conferences and events • Educational webinars and workshops for customer awareness	

COST STRUCTURE	REVENUE STREAM(S)
• Research and development for continuous platform improvement • Salaries for cybersecurity experts, data scientists, and developers • Infrastructure costs for hosting the platform and managing data • Marketing and promotional expenses for customer acquisition • Ongoing maintenance and customer support costs	• Subscription-based model for healthcare institutions and hospitals • Licensing fees for medical device manufacturers • Consulting fees for specialized threat assessment and cybersecurity services

Figure 3 HEIR's Platform Business Model Canvas

3.2.2 HEIR's Visualizations

The term Visualization refers to the process of representing data or information in a visual or graphical format. It involves the creation of visual elements such as charts, graphs, diagrams, and maps to convey complex data in a more accessible and intuitive manner. Graphical User Interfaces (GUIs) are visual interfaces that enable users to interact with software or computer systems using graphical elements such as icons, buttons, menus, and windows. Overall, visualization and GUIs in platforms are designed to simplify complex information and interactions, enabling users to navigate and utilize the platform's capabilities more effectively.

As presented in D7.8 (Exploitation strategy, training material, and activities – P2), which presents a compilation of plans for future exploitation and sustainability of the project results, AEGIS showcased the business potential of the HEIR Visualizations (Graphical User Interfaces) that was used as a basis in the HEIR project, it was applied to all pilot sites and was considered in all use cases.

HEIR's Visualizations Business Model Canvas is available in Figure 4.

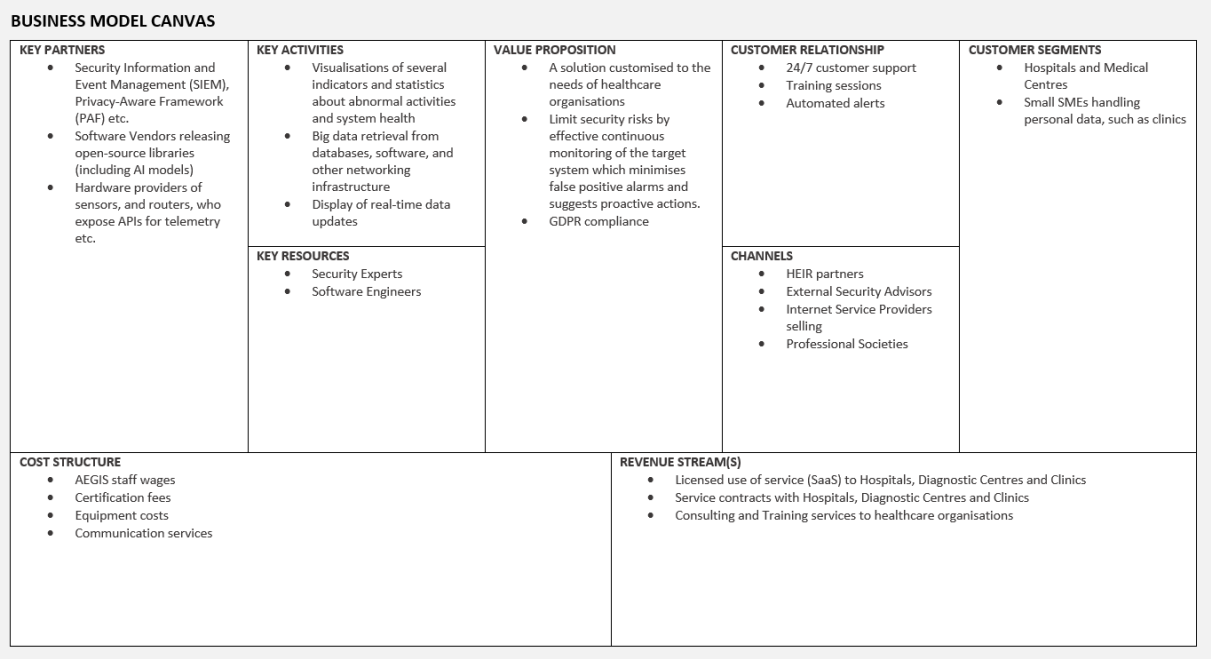


Figure 4 HEIR's Visualization Business Model Canvas

3.2.3 HEIR's Forensics Visualization Toolkit

Digital forensics analysis, also known as computer forensics or cyber forensics, focuses on investigating and analyzing digital devices and electronic evidence to uncover information related to cybercrimes, data breaches, and other digital incidents. It involves the identification, preservation, extraction, and interpretation of data from various digital sources. Digital forensics analysts utilize specialized tools, such as the Forensics Visualization Toolkit (FVT), and techniques to examine digital devices such as computers and network systems.

As presented in D7.8 (Exploitation strategy, training material, and activities – P2), which presents a compilation of plans for future exploitation and sustainability of the project results, AEGIS showcased the business potential of its Forensics Visualization Tool (FVT) that was used as a basis in the HEIR project, it was applied to all pilot sites and was considered in all use cases.

HEIR's FVT Business Model Canvas is available in Figure 5.

BUSINESS MODEL CANVAS

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITION	CUSTOMER RELATIONSHIP	CUSTOMER SEGMENTS
• Providers of Security Information and Event Management (SIEM), Intrusion Detection Systems (IDS), honeypots, etc. • Hardware providers of sensors, and routers, who expose APIs for telemetry etc.	• Forensics analysis: what happened in case of a materialised attack (report) • Calculation of several indicators and statistics about abnormal activities and system health • Limit security risks by effective continuous monitoring of the target system which minimizes false positive alarms and suggests proactive actions • Visualisations of several indicators and statistics about abnormal activities and system health • Telemetry: Big data retrieval from different databases, software, hosts, sensors, and other networking infrastructure	• The ability to "travel back in time" and compare the current situation with similar events that occurred in the past • Adaptation of the displayed information based on previously encountered situations that can be saved for future comparison • Automated workflows reduce mean time to repair (MTTR) • Insightful visualisations help in identifying hidden patterns and reducing false positives/negatives	• 24/7 customer support • Training sessions • Automated alerts • Webinars and presentations to raise awareness	• Hospitals and Medical Centres • Small SMEs handling personal data, such as clinics • Insurance companies • Software providers/integrators
	KEY RESOURCES • Security Experts • Software Engineers		**CHANNELS** • HEIR partners • External Security Advisors • ICT Infor days • Website • Social Media • Exhibitions & Conferences	

COST STRUCTURE	REVENUE STREAM(S)
• AEGIS staff wages • Certification fees • Communication services • Marketing costs	• Licensed use of service (SaaS) from SMEs and Hospitals • Service contracts with Hospitals and Insurance Companies • Consulting and Training services to healthcare organisations

Figure 5 FVT's Business Model Canvas

3.2.4 HEIR's Observatory

Cybersecurity incidents have revealed that the healthcare sector stands as one of the most susceptible to cyberattacks. However, there is currently a deficiency in the establishment of a benchmarking methodology and pertinent Key Performance Indicators (KPIs) for evaluating the cyber-security posture of organizations within specific domains, particularly in the field of healthcare. Simultaneously, the absence of a cohesive platform to monitor the security state of electronic devices and offer real-time forensic analysis within healthcare environments, such as networks of hospitals and medical centers, further compounds the situation.

There is a solution related to healthcare's cybersecurity, the National Cyber Security Index [29], however it does not offer an automated and current overview regarding how a specific organization compares to other entities within its domain, combined with tools for actively monitoring and comprehending a hospital's real-time cybersecurity condition.

The Observatory constitutes a web-based platform accessible to stakeholders, policymakers, and legislators. It encompasses an intelligent knowledge base alongside interactive visualization tools, with the primary aim of illustrating the panorama of cyber threats concerning electronic medical devices. Furthermore, it provides comprehensive insights into detailed cybersecurity assurance levels and their progression over time. The compiled vulnerabilities and security-related data within the Observatory are constituted by the Local RAMA score and metadata derived from the HEIR Clients. Additionally, the expansion of the HEIR ecosystem to encompass more hospitals and medical centers directly correlates with improved outcomes from the Observatory.

HEIR's Observatory Business Model Canvas is available in Figure 6.

[29] https://ncsi.ega.ee/

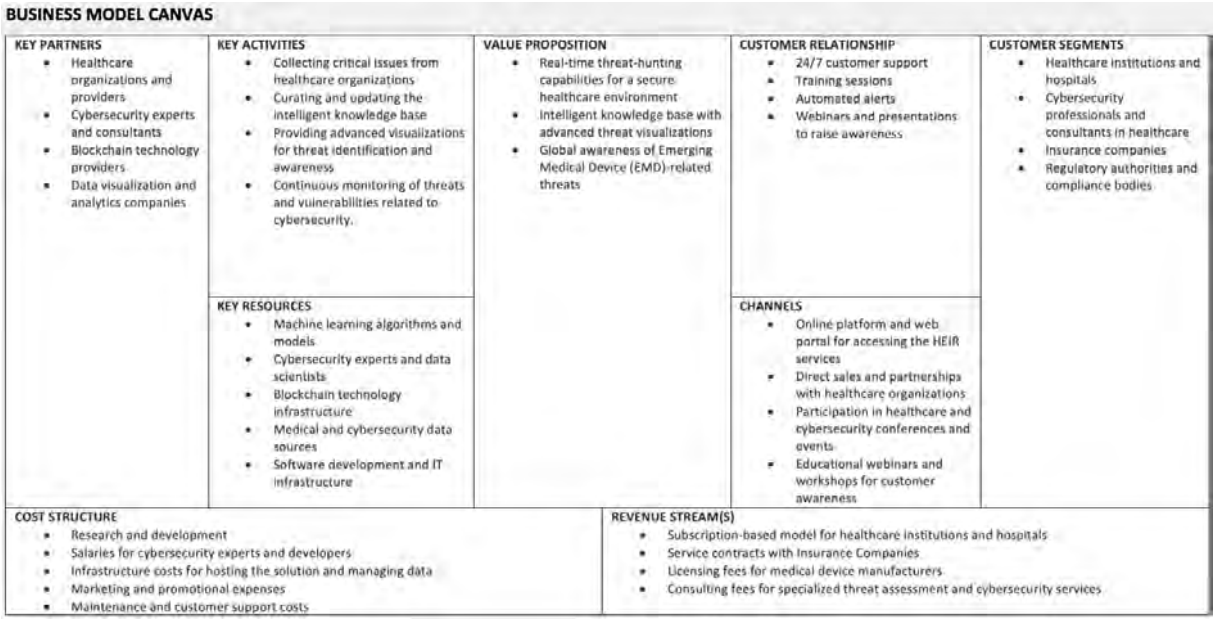


Figure 6 HEIR's Observatory Business Model Canvas

3.2.5 HEIR's Privacy-Aware Framework

As part of HEIR's work on the Privacy Aware Framework (PAF), IBM made significant contributions to its work on the Open Source Fybrik framework (https://fybrik.io/). The Policy Aware Framework builds on Fybrik and therefore, enriching the Fybrik framework was key to improving the PAF.

Fybrik[30] has been released under an Apache 2.0 license and is publicly available. The Fybrik Github repo has numerous examples of how Fybrik can be used in a wide variety of use cases, including a scenario from HEIR's Norwegian Healthcare use case[31] which connects to a backend FHIR server.

During the course of HEIR, IBM and ING collaborated on using Fybrik technology to protect data across multiple clouds[32]. Additionally, during the course of the project, PAF worked closely with the HEIR Norwegian healthcare partners to produce a number of prototype solutions which addressed real-word data sharing issues that they had, such as demonstrating how PAF could be used to seamlessly federate disparate healthcare registries which providing privacy-driven access control to the data. This technology was presented to both the technical and medical staff for the other HEIR use case partners, namely in the Croydon, PAGNI and Hygea hospitals. In all cases, the presentation was well received, and drew a lot of interest. A video explaining the potential of HEIR PAF technology in the world of healthcare was produced and made available on YouTube[33].

[30] https://github.com/fybrik/fybrik
[31] https://github.com/fybrik/REST-read-example
[32] https://medium.com/fybrik/how-ing-and-ibm-are-collaborating-to-manage-enterprise-data-across-multiple-clouds-2f5d6d48963d
[33] https://www.youtube.com/watch?v=gCeD78pAzwE&list=PLQvL7sLaqUACCPXoYi5Mo60Icz9avTRnN&index=4

Based on the positive evaluation of PAF technology in the HEIR use cases, from a business perspective, PAF and Fybrik technology developed in HEIR have the potential to be used future IBM cloud offerings.

HEIR's PAF Business Model Canvas is available in Figure 7.

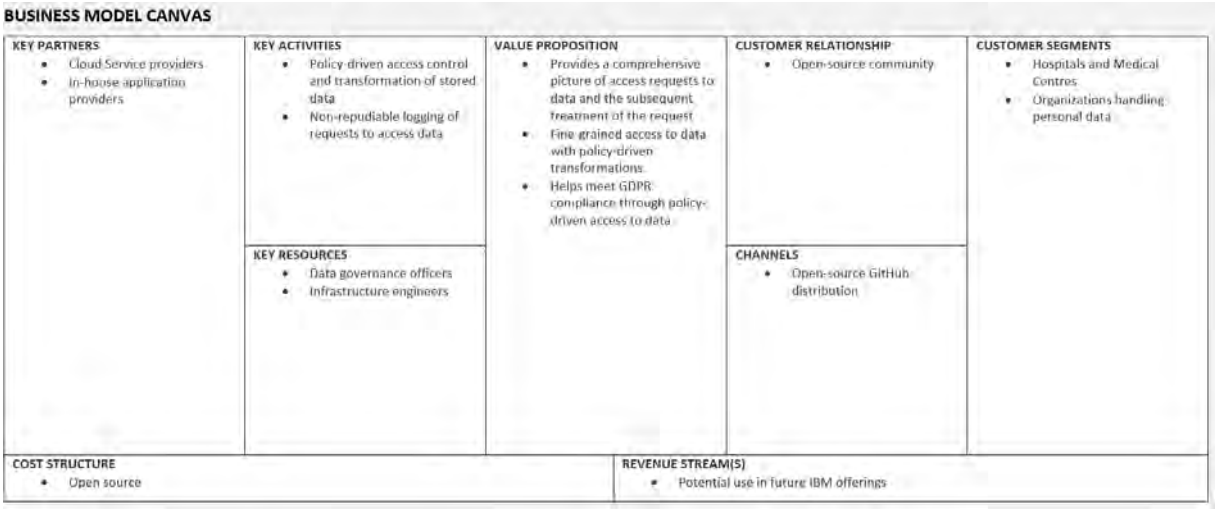


Figure 7 HEIR's PAF Business Model Canvas

3.2.6 Blockchain-based Auditing Mechanism

Auditing mechanisms play a crucial role in addressing the problem of trust, transparency, and accountability in various domains. Traditional auditing processes often suffer from inefficiencies, lack of transparency, and the potential for manipulation or fraud. In the context of HEIR project, the goal is to provide an immutable record of all data access attempts, a filtering mechanism to identify malicious unauthorized access attempts on a regular (daily, weekly, monthly etc.) basis, and a timeline of events in the form of abnormal data access requests, facilitating the trace of malicious user behaviors back in time. The unique selling proposition of the suggested in blockchain-based solution that tackles this challenge, is built on the following advantages: (1) immutability and transparency; (2) decentralization; (3) enhanced data integrity; (4) real-time auditing and continuous monitoring; (5) smart contracts support and corresponding automations; (6) enhanced privacy and confidentiality and (7) cost-efficiency.

The business scalability of this mechanism is ensured through the adoption of a BaaS adoption, enabling the provision of such features on-demand, and as a part of a larger security suite of services. Taking into account the market trends presented in the previous section, it becomes evident that that a fertile business ground exists for commercially successful blockchain based auditing and transparency mechanism in the healthcare domain. As this market enters in its development curve, the main steps (0.5 – 2 years from now) towards this direction include the organization of additional pilot activities, in order to refine our value proposition, test our business hypothesis and define in detail our sweet-spot of customer segments, that will enable the scaling of the suggested solution and the development of traction.

HEIR's Blockchain-based auditing mechanism Business Model Canvas is available in Figure 8.

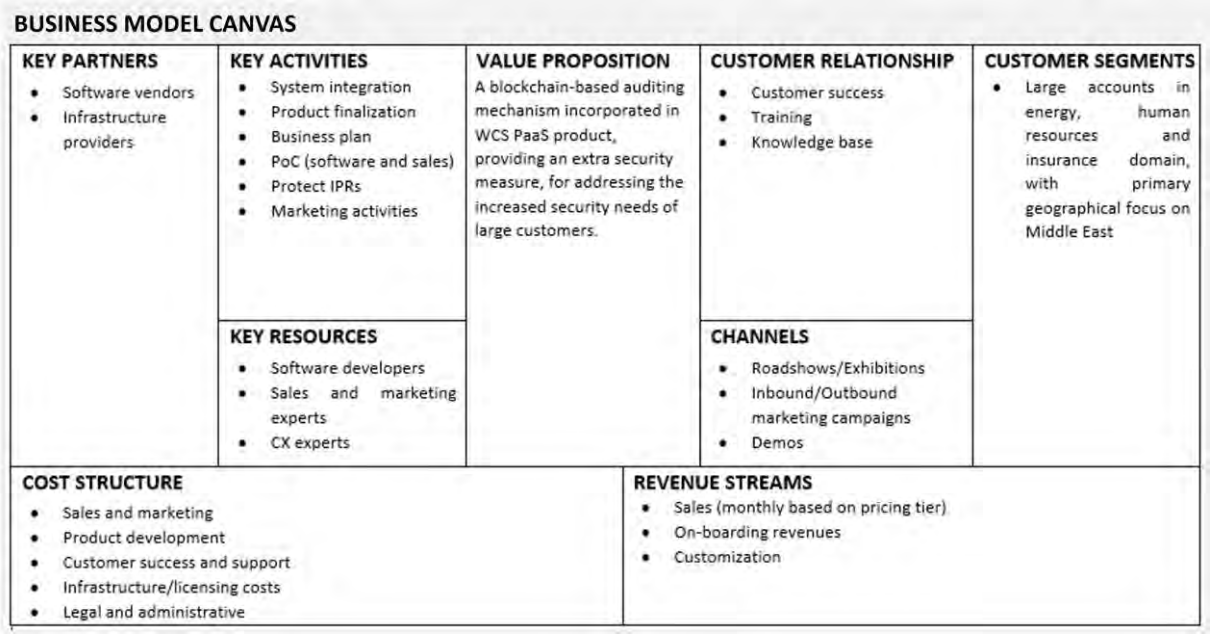


Figure 8 HEIR's Blockchain-based auditing mechanism Business Model Canvas

3.2.7 HEIR's SIEM System

Real-time threat monitoring is a critical component of modern business security strategies. It involves the continuous monitoring and analysis of various data sources to identify and respond to potential threats and security breaches in real-time. This analysis aims to assess the key aspects of real-time threat monitoring from a business perspective.

The market for real-time threat monitoring has experienced significant growth in recent years due to the increasing frequency and sophistication of cyber threats. Organizations across various sectors, including finance, healthcare, and e-commerce, recognize the importance of proactive threat detection and prevention. The market is highly competitive, with several established players and emerging startups offering real-time threat-monitoring solutions.

Real-time threat monitoring provides numerous benefits to organizations. Firstly, Early Threat Detection gives the ability to monitor and analyze data in real-time, and therefore businesses can identify potential threats and security breaches as they occur, enabling swift response and mitigation. Secondly, Proactive Incident Response enables organizations to proactively respond to security incidents, minimizing the impact and reducing recovery time through real-time threat monitoring. Compliance with data protection and privacy regulations is crucial for businesses. Real-time threat monitoring helps ensure compliance by detecting and addressing vulnerabilities and potential non-compliant activities promptly, forming an Enhanced Compliance regime. Additionally, real-time threat monitoring can ensure the Protection of Reputation by preventing security breaches and minimizing the impact of incidents, safeguarding a business's reputation and instilling trust among customers and partners. Last but not least, timely detection and response to threats can significantly reduce the financial impact of security incidents, resulting in Cost Savings. According to a report by Accenture, organizations that leverage advanced threat intelligence and real-time monitoring experience an average cost savings of $2.8 million in cyberattack costs compared to those without such capabilities (Accenture, 2021). All of the above constitute a set of key parameters to be taken into account by organizations before choosing a SIEM solution for their application. The HEIR SIEM offers these benefits, illustrating an important advancement for real-time threat monitoring in the healthcare sector.

The valuable benefits offered to organizations are established through the key features and functionality owned by the unique nature of real-time threat monitoring. Log and Event Analysis is the first key functionality, which offers the monitoring and analysis of log files, system events, and network traffic to identify anomalies and suspicious activities. Furthermore, Behavioral Analytics introduces the utilization of machine learning and artificial intelligence techniques to detect patterns and anomalies in user behaviour, network traffic, and system activities. Furthermore, Threat Intelligence Integration enables the integration with external threat intelligence feeds to enhance detection capabilities by leveraging up-to-date information on emerging threats. In terms of Incident Response Automation, integration between incident response workflows and automation of response actions can significantly minimize manual effort and response time. Additionally, Real-time Alerts and Notifications provide instant alerts and notifications to security teams or administrators when potential threats are detected, allowing for immediate action. Finally, interactive dashboards and comprehensive reports are part of the Visualization and Reporting feature, that provide visibility into the security posture of the organization, including threat trends and incident statistics. When implementing real-time threat monitoring, it is vital that organizations take into account several implementation considerations based on specific factors. One such factor is Scalability, implying that the solution should be scalable to handle the increasing volume of data generated by the organization's systems and networks. Integration Capabilities are another factor to consider when implementing real-time threat monitoring, as it involves the integration with existing security infrastructure, such as firewalls, intrusion detection systems, and SIEM platforms, which is crucial for effective threat monitoring. In addition, Data Privacy and Compliance are important to be implemented. Organizations need to ensure that the solution adheres to data privacy regulations and handles sensitive information appropriately. Similarly, Skill Requirements are required, as adequate resources with the necessary skills and expertise in threat monitoring and incident response should be available to operate and manage the system effectively. Lastly, regular updates, patches, and maintenance are essential to keep the threat monitoring system effective against evolving threats, which correspond to Ongoing Maintenance and Updates.

When investing in real-time threat-monitoring technologies, organizations should consider and carry out the necessary research and analysis regarding the Return on Investment (ROI) and costs justification. Calculating the ROI for real-time threat monitoring involves considering both the potential cost savings from mitigated security incidents and the value of safeguarding the organization's reputation and customer trust. Organizations should compare the costs of implementing and operating a real-time threat monitoring solution against potential financial losses, regulatory fines, and reputational damage associated with security breaches.

As presented in D7.8 (Exploitation strategy, training material, and activities – P2), which presents a compilation of plans for future exploitation and sustainability of the project results, ITML showcased the business potential of its SIEM software product that was used as a basis in the HEIR project and was applied to all pilot sites. Specifically, the SIEM has been successfully integrated into HEIR’s MVP, HEIR’s 1st prototype, and HEIR’s integrated solution, and it is solely responsible for collecting all the information portrayed in the Forensics Visualization Toolkit (FVT) GUI. It has been deployed in all pilots and was considered in all use cases. Through an intuitive, single pane of glass monitoring, several ready-made integrations are provided, including BitDefender antivirus and firewall , Symantec DLP , FortiGate firewall , and an ever-growing list of market-leading software solutions. HEIR SIEM also provides out-of-the-box reports, alerts, and compliance capabilities, while being extensible to adapt to any IT infrastructure: on-prem, cloud, or

hybrid. The fact that this tool is fully customizable and can be tailored to meet the specific needs and requirements of an organization to fit specific business processes, workflows, and data structures, and can be easily integrated with other systems or applications and tools, enables its exploitation by various organizations in the healthcare, energy, and manufacturing, sectors considering Security Monitoring, Log Management, Threat Detection and Response, Incident Management, Compliance, and Audit, adding value to the business operations while safeguarding their important assets from cyberattacks.

The value proposition of the HEIR SIEM revolves around its ability to strengthen security posture, enable proactive incident response, provide situational awareness, optimize resource utilization, ensure compliance, and leverage continuous threat intelligence. By investing in such tools, organizations can bolster their defenses and stay ahead of the ever-evolving threat landscape.

HEIR's SIEM System's Business Model Canvas is available in Figure 9.

BUSINESS MODEL CANVAS

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITION	CUSTOMER RELATIONSHIP	CUSTOMER SEGMENTS
• Cybersecurity technology providers for access to cutting-edge tools • Data providers for up-to-date threat intelligence • Resellers and distributors to reach a broader customer base • Privacy and ethics experts • Cybersecurity consulting firms and IT service providers for referrals.	• Continuous monitoring of threats and vulnerabilities related to cybersecurity. • Incident analysis and response in real-time • Customer support and relationship management • Research and development to improve threat detection capabilities **KEY RESOURCES** • Skilled cybersecurity analysts, experts, and technical staff • Proprietary threat intelligence and monitoring tools • Reliable IT infrastructure and data centres • Partnerships with cybersecurity technology providers	• Real-time threat detection and monitoring to prevent cyber-attacks. • Early warning and notification system to respond quickly to potential threats • Customizable threat monitoring solutions tailored to each customer's needs • 24/7 security operations centre (SOC) support for immediate assistance	• Personalised onboarding and setup assistance • Regular check-ins and updates on the threat landscape • Efficient customer support and incident response • Educational resources and webinars to help customers improve their security posture **CHANNELS** • Online marketing and advertising • Direct sales and partnerships with cybersecurity firms • Participation in industry events and conferences • Referral programs from existing customers	• Small and Medium-sized Businesses (SMBs) • Enterprises • Government organizations • Critical infrastructure providers • Non-profit organizations

COST STRUCTURE	REVENUE STREAM(S)
• Personnel costs • Infrastructure and technology investments • Marketing and promotional expenses	• Subscription-based pricing models • Tiered pricing based on the level of threat monitoring and support required. • One-time setup and implementation fee.

Figure 9 HEIR's SIEM System's Business Model Canvas

3.2.8 HEIR's Aggregator

The HEIR Aggregator serves as a connecting component within the HEIR healthcare cybersecurity ecosystem. It collects and consolidates data generated by HEIR clients and the RAMA calculator, orchestrating their transmission to HEIR's 1st Layer GUI and the Observatory. This dynamic liaison enhances real-time situational awareness, streamlines cybersecurity workflows, and offers improved data privacy and compliance measures. With a versatile architecture deployed through Docker containers in Kubernetes, supported by Python libraries, the Aggregator embodies efficient data handling and communication. It has evolved from a department-specific solution to a universal connecting hub across participant Pilots, actively participating in safeguarding healthcare institutions' digital security.

HEIR's Aggregator Business Model Canvas is available in Figure 10.

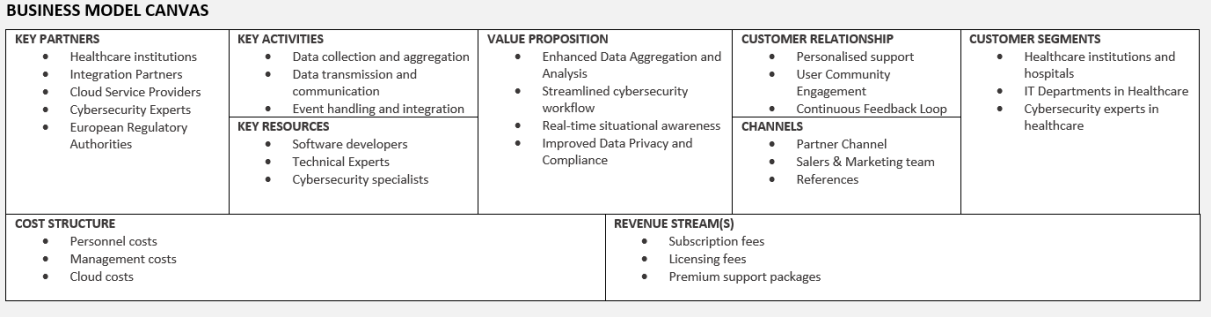


Figure 10 HEIR's Aggregator Business Model Canvas.

3.2.9 HEIR's Local and Global RAMA score

Although the healthcare sector has been capitalizing on digital advancements to improve patient outcomes and experiences substantially, poor security practices are still heavily used. Poor computer and user account security, remote access and home working, and lack of encryption are critical issues in the healthcare sector. These, in combination with the lack of up-to-date risk assessment techniques and security awareness, have led the healthcare sector to be one of the most impacted in terms of average data breach cost, as well as be the sector that faces the most significant influx of cyber-attacks, regarding both volume (69%) and complexity (67%). HEIR advances the state-of-the-art by proposing a novel Risk Assessment for Medical Applications (RAMA) score, which acts as a benchmark and estimates medical devices' attack surface and resilience by incorporating several critical issues. The Local and Global RAMA Score incorporates several critical issues reported by a centralized client and estimates the attack surface and the resilience of the underlying medical devices per healthcare organization.

HEIR's Local and Global RAMA score Business Model Canvas is available in Figure 11.

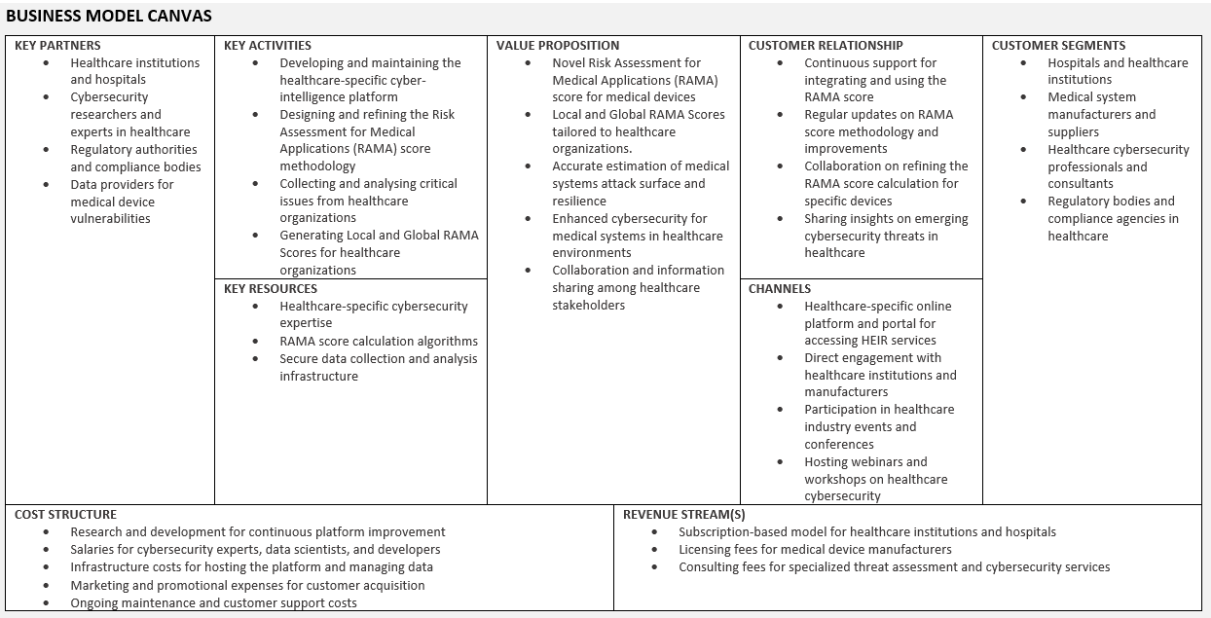


Figure 11 HEIR's Local and Global RAMA score Business Model Canvas

3.2.10 Security and Privacy Assurance (SPA) Suite

SPHYNX's Security and Privacy Assurance Suite can satisfy your industrial infrastructure's needs for

- Complementary assessments (e.g., vulnerability assessment, penetration testing, monitoring, existing certificates)
- Hybrid assessments, combining outcomes of individual assessments; but, how to handle complementary outcomes & conflicting outcomes?
- Incremental assessments & automated adaptation and evolution of assessment schemes
- Automated assessments
    - For all levels of risk (system, business processes & mission, organizational)
    - For all horizons of risk management (tactical short term, tactical medium term & strategic

The novel security assurance platform offers:

- Hybrid security and privacy assessments that include and combine automated threat and vulnerability analysis, static analysis, penetration testing and continuous runtime monitoring to provide a comprehensive and multi perspective analysis of the security and privacy posture of an enterprise and its systems.
- Effective and comprehensive threat information exchange
- Enhanced analytics & automation for establishing the S&P posture of an organization.
- "Out-of-the-box thinking" and support S&P risk management.
- Efficient Interoperability with the rest of the COLLABS components/services
- Interoperability with third-party system platforms and programmatic connectivity to different systems through appropriate probes (e.g., event captors, test tools) that enable it to obtain the monitoring and/or test evidence required for assurance and/or certification assessments.
- Sophisticated event processing capabilities that can realize complex signature or anomaly-based assessments.
- Model driven customizations to enable the realization of different security standards and risk management requirements.
- Advanced and customizable reporting for audit purposes

Security and Privacy Assurance Suite's Business Model Canvas is available in Figure 12.

BUSINESS MODEL CANVAS

<table>
<tr>
<td rowspan="2">KEY PARTNERS
Industrial companies and organizations with complex infrastructure
Cybersecurity experts and consultants
Providers of vulnerability assessment tools
Providers of penetration testing services
Organizations offering existing security certificates
Third-party system platforms and event capture tools</td>
<td>KEY ACTIVITIES
Development and maintenance of the Security and Privacy Assurance Suite
Conducting complementary assessments, vulnerability assessments, penetration testing, and monitoring
Integration of outcomes from various assessments, handling conflicting outcomes
Automation of assessment schemes and continuous adaptation
Implementation of automated assessments for different risk levels and horizons
Enhancing analytics and automation for security and privacy posture evaluation</td>
<td rowspan="2">VALUE PROPOSITION
Comprehensive hybrid security and privacy assessments
Effective threat information exchange
Enhanced analytics and automation for security posture assessment
Support for "out-of-the-box thinking" in security and privacy risk management.
Interoperability with other COLLABS components/services
Connectivity with third-party systems for evidence collection
Sophisticated event processing capabilities for complex assessments
Customization for different security standards and risk requirements
Advanced and customizable reporting for audits</td>
<td>CUSTOMER RELATIONSHIP
Technical support for platform implementation and usage
Continuous updates and improvements based on evolving threats and standards
Customization of assessments to fit specific organizational needs
Collaboration on resolving conflicting assessment outcomes
Training and workshops on using the Security and Privacy Assurance Suite</td>
<td rowspan="2">CUSTOMER SEGMENTS
Industrial organizations with complex infrastructure
Cybersecurity teams and professionals
Compliance and certification authorities
Third-party system platforms seeking assurance and certification</td>
</tr>
<tr>
<td>KEY RESOURCES
Advanced threat and vulnerability analysis tools
Penetration testing tools and expertise
Runtime monitoring technologies
Integration and automation frameworks
Expertise in security standards and risk management
Model-driven customization capabilities</td>
<td>CHANNELS
Online platform for accessing the Security and Privacy Assurance Suite
Direct sales and partnerships with industrial organizations
Participation in cybersecurity conferences and industry events
Training sessions and webinars for customer awareness</td>
</tr>
<tr>
<td colspan="3">COST STRUCTURE
Research and development for ongoing platform enhancement
Salaries for cybersecurity experts and software developers
Infrastructure costs for hosting the platform and managing data
Marketing and promotional expenses for customer acquisition
Ongoing maintenance and customer support costs</td>
<td colspan="3">REVENUE STREAM(S)
Licensing fees for industrial organizations using the suite
Subscription-based model for continuous updates and support
Consulting fees for specialized assessment customization and interpretation
Revenue from integration with third-party system platforms</td>
</tr>
</table>

Figure 12 Security and Privacy Assurance Suite's Business Model Canvas

3.2.11 HEIR's Client

The use of un-synced services and solutions comes without the adaptability required by very different healthcare landscapes i.e., each European country has its own regulatory policies, and each healthcare unit has its own hardware and software infrastructure forcing the professionals to navigate a very complex landscape to obtain minimum cybersecurity.

The **HEIR Client**, developed by Bitdefender team, includes the following assets:

- Heir Network Module - Network monitoring and detection
- Heir Threat Detection Module - Anti Malware
- Heir Exploit Tester - Risk assessment
- Heir Vulnerability Assessment - Risk assessment
- Heir Cryptographic Checker – Risk assessment

The HEIR Client offers (i) Unified security and analytics for various environments with easy administration; (ii) Advanced threat intelligence built-in based on collaborating with project pilots and academia; (iii) Better return on investment determined by engineering the complexity out of security, to reduce risk at a lower total cost.

HEIR's Client Business Model Canvas is available in Figure 13.

BUSINESS MODEL CANVAS

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITION	CUSTOMER RELATIONSHIP	CUSTOMER SEGMENTS
• Existing B2B22B and B2B commercial partners • Healthcare institutions and hospitals • Cybersecurity researchers and experts in addressing specific challenges within the healthcare environment • Regulatory authorities and compliance bodies dealing with cybersecurity for health • Data providers for medical device vulnerabilities	• Collecting and analysing critical issues from healthcare organisations • Refining and maintaining the healthcare-specific module and its components • Piloting the HEIR Client deployment in various healthcare environments **KEY RESOURCES** • Cybersecurity experts • Software Engineers • Product Managers	• A solution customised to the needs of healthcare organisations • Comprehensive hybrid security and privacy assessments • Customisation for different security standards and risk requirements • Connectivity with third-party systems for evidence collection	• Healthcare institutions and hospitals • Medical device manufacturers • Cybersecurity professionals and consultants in healthcare **CHANNELS** • BD online page and web portal for accessing the HEIR solutions • Direct sales and partnerships with healthcare organisations • Thematic events	• Healthcare institutions and hospitals • Medical device manufacturers • Cybersecurity professionals and consultants in healthcare • Regulatory authorities and compliance bodies

COST STRUCTURE	REVENUE STREAM(S)
• BD personnel cost • Marketing cost • Equipment cost	• Licensed use of services (SaaS) for healthcare organisations for the BD GravityZone suite, including the HEIR Client • Revenue share from the B2B2B and B2B commercial partnerships

Figure 13 HEIR's Client Business Model Canvas

3.2.12 Anomaly Detection

The HEIR Platform offers a comprehensive solution for efficient event and threat data classification tailored to meet health systems' complex cyber security requirements and criticality levels. At the platform's core lies the Anomaly Detection module, leveraging state-of-the-art machine learning (ML) models and tailored adaptations of existing algorithms. This module plays a pivotal role in the rapid digitalization of healthcare records, IoT devices, and interconnected systems, providing a proactive approach to swiftly detect and respond to abnormal activities that could signify cyber threats or unusual behavior.

Anomaly detection has emerged as a crucial tool within the healthcare sector, revolutionizing how healthcare organizations identify and mitigate potential threats to patient data and critical infrastructure. With the global machine-learning market projected to reach $305.62 billion by 2030, anomaly detection techniques offer a proactive approach to swiftly detect and respond to abnormal activities that could signify cyber threats or unusual behavior.

Combining specific rules and novel ML models, the Anomaly Detection module intelligently classifies threat data, enabling health systems to respond proactively to potential security breaches. The module's versatility is exemplified by its capability to tailor the selected ML model or algorithm to the specific use case, whether supervised or unsupervised learning, as demonstrated by the successful implementations in two prominent use cases - PAGNI and CROYDON (in D2.3 and D5.5).

The adaptability and scalability of the Anomaly Detection module within the HEIR platform empower health systems with tangible and visually represented results via the FVT toolkit. The module's ability to effectively identify and prioritize cyber threats enhances the overall cyber security posture, making the HEIR platform a transformative solution for the healthcare industry.

As healthcare organizations continue to embrace digital transformation and data-driven decision-making, the importance of robust anomaly detection solutions will only grow, marking a significant step towards ensuring a safe and secure healthcare ecosystem in the face of evolving cyber threats. With anomaly detection playing a pivotal role in safeguarding sensitive information and ensuring uninterrupted operations, the HEIR platform delivers comprehensive and tailored cybersecurity solutions to safeguard health systems and essential services in an increasingly digitized world.

HEIR's Anomaly Detection Business Model Canvas is available in Figure 14.

<table>
<tr>
<td rowspan="2">KEY PARTNERS
• Cybersecurity Experts
• Healthcare Institutions and Hospitals
• Data Providers
• Medical Device Manufacturers
• Academic Institutions</td>
<td>KEY ACTIVITIES
• Algorithm Development and Optimization
• Model Training and Data Pre-processing
• Domain Specific Customization
• Collaboration with Partners
• Compliance with Security Measurements
• Continuous Monitoring</td>
<td rowspan="2">VALUE PROPOSITION
• Advanced Anomaly Detection and Threat Classification
• Customized Solution for Healthcare Security
• Real-Time Monitoring and Early Threat Detection</td>
<td>CUSTOMER RELATIONSHIP
• Personalised Support and Training
• Collaborative Partnership
• Continuous Feedback Loop
• Continuous Knowledge Sharing</td>
<td rowspan="2">CUSTOMER SEGMENTS
• Healthcare Institutions and Hospitals
• IT Departments in Healthcare
• Cybersecurity solution Providers
• Medical Device Manufacturers</td>
</tr>
<tr>
<td>KEY RESOURCES
• Machine Learning Experts
• Technical Experts
• Cybersecurity Experts
• Access to High-quality Data
• Partnerships and Collaborations</td>
<td>CHANNELS
• Partnership Collaboration
• Direct Sales and Marketing
• Online Platforms and Webinars</td>
</tr>
<tr>
<td colspan="2">COST STRUCTURE
• Research and Development
• Partnership and Collaboration Expenses
• Data Acquisition and Management Costs</td>
<td colspan="3">REVENUE STREAM(S)
• Subscription Model
• Licensing Fees
• Professional Services</td>
</tr>
</table>

Figure 14 HEIR's Anomaly Detection Business Model Canvas

3.2.13 GPU Cluster with SGX Support

The business potential of GPU clusters with Intel SGX support is poised to revolutionize the landscape of data processing and security across various industries. By integrating Intel's SGX technology, FORTH's solution offers outstanding hardware-based memory encryption and isolation, establishing secure enclaves that shield sensitive data from potential breaches. This level of security is especially crucial in today's world, where data breaches and cyberattacks are becoming increasingly sophisticated.

Deployed within HEIR, GPU cluster can be used to train the anomaly detection module especially in cases where the trained data is sensitive and cannot be leaked. More specifically, the commodity cluster of GPUs, working together in parallel, delivers unparalleled computational power. AI/ML applications can harness the full potential of the GPU cluster to train complex models and process massive datasets efficiently, leading to more accurate predictions and faster insights.

In conclusion, the business potential of GPU clusters with Intel SGX support is multi-faceted and highly promising. The integration of SGX technology ensures unparalleled security for sensitive data, making it ideal for industries that prioritize data privacy and protection. The exceptional performance capabilities of the commodity GPU cluster cater to data-intensive tasks, while its tailored approach provides customized solutions for various sectors. As the demand for secure and high-performance data processing continues to grow, FORTH's GPU cluster with SGX support positions itself as a cutting-edge and reliable solution for businesses across healthcare, finance, research, and beyond.

GPU Cluster with SGX Support's Business Model Canvas is available in Figure 15.

BUSINESS MODEL CANVAS

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITION	CUSTOMER RELATIONSHIP	CUSTOMER SEGMENTS
• Intel and hardware technology providers • Data privacy and compliance consultants • Industry associations and organizations	• Research and development for integrating SGX technology • Customization for GPU clusters for different industries **KEY RESOURCES** • SGX technology expertise • GPU hardware suppliers • Skilled technical team for support and customization • Marketing and sales personnel	• Data security via Intel SGX technology to provide hardware-based memory encryption. • High-performance computing through a cluster of GPUs • Scalable infrastructure that can accommodate increasing workloads and demands without compromising performance • Competitive advantage by providing industries with a strategic edge by combining security, performance, and customization	• 24/7 customer support • Training sessions • Regular newsletters and updates for customer engagements **CHANNELS** • HEIR partners • External Security Advisors • Professional Societies	• Healthcare institutions (for secure patient data processing) • Financial organizations (for secure financial data processing) • Research institutions and laboratories (for secure research data processing) • AI/ML companies (for high-performance data processing)

COST STRUCTURE	REVENUE STREAM(S)
• Research and development costs • Hardware procurement and assembly • Employee salaries and benefits • Customer support and maintenance	• Software license for SGX Integration and management • Maintenance and support subscriptions

Figure 15 GPU Cluster with SGX Support's Business Model Canvas

4. The HEIR Marketplace

The HEIR Marketplace serves as a comprehensive representation of the broader HEIR platform, offering a meticulous breakdown of its multifaceted components, security enhancements, and distinctive merits. This platform diligently addresses critical security needs by implementing robust measures to safeguard healthcare organizations.

Within the HEIR Marketplace, each component is meticulously expounded upon, revealing (a) the problem they are trying to solve, (b) the solution they offer, and (c) its unique value proposition. These components not only elevate the protection of sensitive archival content but also lay the foundation for an innovative and secure environment. Their novel features are meticulously detailed, showcasing their potential to foster collaboration, streamline access, and facilitate seamless transactions.

Furthermore, the HEIR Marketplace's portrayal of the individual components includes a comprehensive depiction of how each addresses distinct security requirements. This granular insight highlights the platform's commitment to ensuring data integrity, thwarting unauthorized access, and upholding stringent privacy standards. Overall, the HEIR Marketplace spotlights the advantages each component offers.

In essence, the HEIR Marketplace functions as an illuminating portal that not only encapsulates the multifaceted nature of the HEIR platform but also underscores its dedication to fostering a secure, collaborative, and transformative space for healthcare organizations.

The HEIR Marketplace (see Figure 16) is accessible through HEIR's official website.[34]

[34] https://heir2020.eu/marketplace/

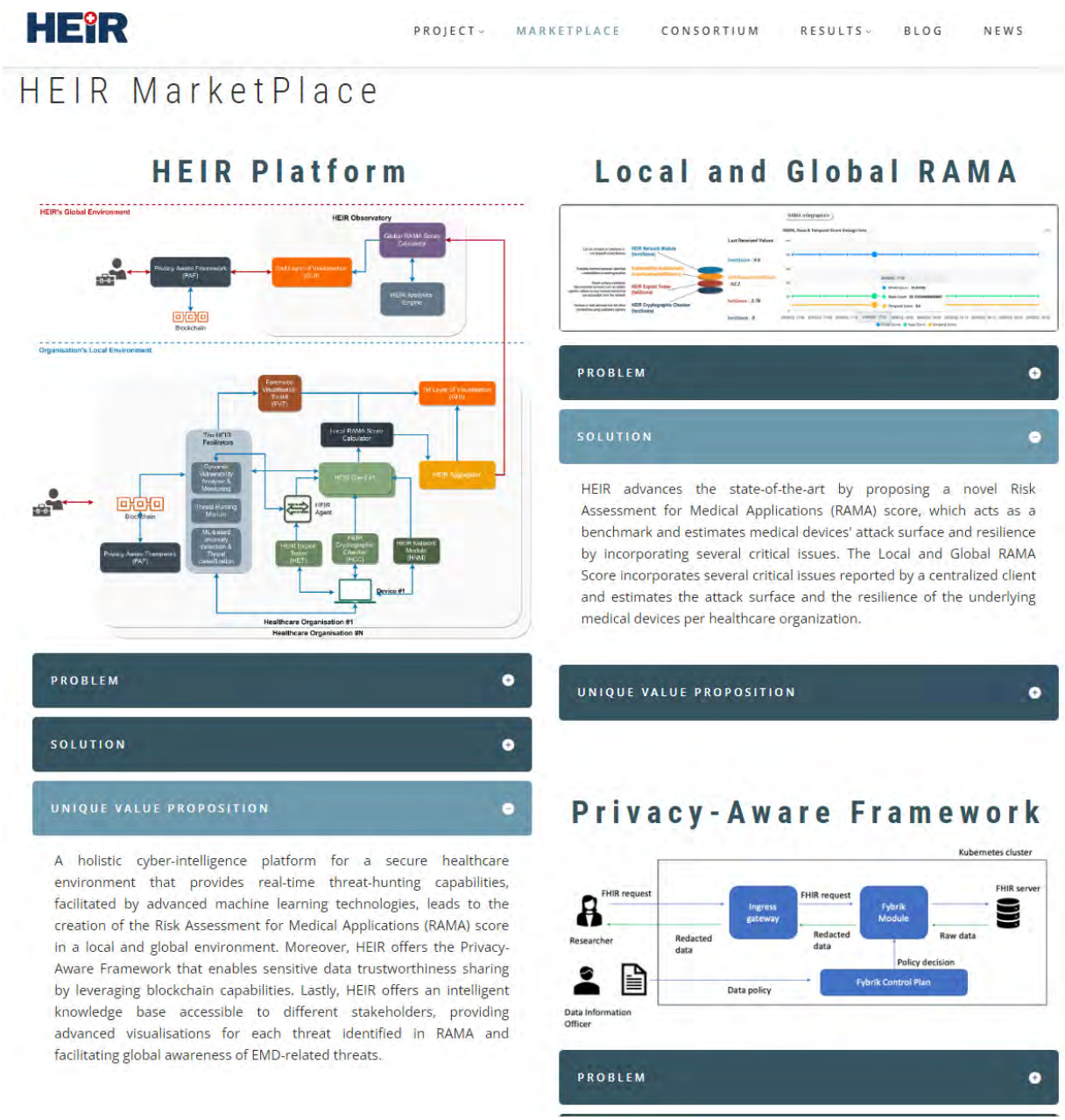


Figure 16 HEIR's Marketplace

5. HEIR Targeted Market and Stakeholders Analysis

5.1 HEIR Targeted Market

The healthcare organizations functioning in the quickly changing healthcare sector make up the targeted market for HEIR. Healthcare providers face tough cybersecurity issues as a result of the increased digitization of medical records, the emergence of linked medical devices, and the expanding threat landscape. Through the provision of a customized cybersecurity platform created especially for the healthcare industry, HEIR seeks to address these issues. The main goal of HEIR is to deliver sophisticated threat detection, anomaly detection, security scoring, and visualization approaches to hospitals, clinics, healthcare networks, and other healthcare providers to preserve patient data, safeguard crucial systems, and assure regulatory compliance.

At the European level, where strict data protection laws like the General Data Protection Regulation (GDPR) govern the privacy and security of personal health information, healthcare institutions are among the target markets for HEIR. Healthcare providers place a high importance on adhering to these rules, and HEIR offers itself as a reliable solution that complies with European data privacy laws. By concentrating on the European market, HEIR hopes to assist healthcare companies in adhering to legal requirements, reducing cyber threats, and fostering trust in their capacity to safeguard private patient information.

Healthcare institutions that make use of the Internet of Medical Things (IoMT) are also included in HEIR's target market. The security threats posed by the IoMT are becoming more noticeable as the healthcare sector embraces connected medical devices more and more. To monitor and secure the network of connected devices, HEIR provides unique threat detection capabilities in recognition of the dynamic threat environment. HEIR intends to offer complete security against potential cyber threats by focusing on healthcare firms using the IoMT. These risks could jeopardize the integrity and confidentiality of patient data and interfere with vital healthcare operations.

Healthcare organizations of various sizes and types, such as large hospital systems, regional healthcare networks, specialty clinics, and individual healthcare practitioners, are included in the market HEIR is targeting. Regardless of size or complexity, HEIR's flexible and adaptable platform can be tailored to meet the specific requirements of each organization. HEIR seeks to make its cybersecurity solution usable and successful for a wide spectrum of healthcare industry stakeholders by focusing on a variety of healthcare organizations. The market that HEIR can target includes healthcare organizations of various sizes and types, including large hospital systems, regional healthcare networks, specialist clinics, and individual healthcare practitioners. Regardless of size or complexity, HEIR's versatile and adaptable platform can be customized to fit any organization's unique needs. By concentrating on various healthcare businesses, HEIR aims to make its cybersecurity solution useful and effective for a broad spectrum of healthcare industry players.

Healthcare institutions that value thorough visualization methods and reporting capabilities are also included in HEIR's target market. Healthcare providers must be able to extract useful insights from cybersecurity data to allocate resources wisely and make informed decisions. The platform from HEIR delivers user-friendly visualization tools and thorough reports that give healthcare businesses a comprehensive understanding of their cybersecurity posture. HEIR seeks to promote educated decision-making for improved security measures by focusing on healthcare companies in need of extensive visualization and reporting tools. This will help in the interpretation of complicated cybersecurity data.

By targeting the healthcare organizations operating within the European market, focusing on the IoMT ecosystem, accommodating diverse organization sizes and types, catering to proactive cybersecurity approaches, and emphasizing comprehensive visualization techniques and reporting capabilities, HEIR aims to establish a strong presence and deliver tailored cybersecurity solutions that meet the specific needs of healthcare providers in their ongoing battle against cyber threats.

5.2 HEIR Stakeholders

The success of the HEIR project relies on engaging and addressing the needs of various key stakeholders within the healthcare industry. These stakeholders encompass healthcare executives and administrators, Chief Information Security Officers (CISOs) and IT security professionals, medical and IT staff, regulatory authorities, and patients and patient advocacy groups. Each stakeholder group plays a vital role in shaping the direction and adoption of the HEIR cybersecurity platform. By understanding their unique perspectives, priorities, and challenges, HEIR aims to deliver a tailored solution that effectively safeguards patient data, protects critical healthcare systems, ensures regulatory compliance, and builds trust among all stakeholders involved in the healthcare ecosystem.

Healthcare Executives and Administrators: Healthcare executives and administrators play a critical role as stakeholders in the HEIR project. They are responsible for the overall management and strategic decision-making within healthcare organizations. These stakeholders are concerned with the protection of patient data, ensuring compliance with regulations, and maintaining the operational continuity of healthcare systems. HEIR offers advanced cybersecurity capabilities that align with their priorities, providing them with the necessary tools to mitigate cyber risks, make informed decisions, and safeguard the reputation and integrity of their organizations.

Chief Information Security Officers (CISOs) and **IT Security Professionals**: CISOs and IT security professionals are key stakeholders for the HEIR project. Their primary responsibility is to manage and secure the IT infrastructure and systems within healthcare organizations. They are focused on identifying potential vulnerabilities, detecting and responding to threats, and implementing robust cybersecurity measures. HEIR offers a tailored cybersecurity platform that supports these professionals in their efforts by providing comprehensive threat detection, anomaly detection, and security scoring capabilities. HEIR enables CISOs and IT security professionals to enhance their organizations' cybersecurity posture and protect critical healthcare systems and patient data.

Medical and IT Staff: Medical and IT staff within healthcare organizations are important stakeholders in the HEIR project. Medical staff, including doctors, nurses, and technicians, rely on secure and uninterrupted access to patient information and medical systems for providing quality care. IT staff, including network administrators and support personnel, are responsible for maintaining and securing the IT infrastructure. HEIR's cybersecurity platform directly impacts these stakeholders by ensuring the availability, integrity, and confidentiality of medical systems and patient data. By targeting these stakeholders, HEIR aims to empower medical and IT staff with the necessary tools to effectively combat cyber threats and focus on delivering quality healthcare services.

Regulatory Authorities: Regulatory authorities, such as healthcare governing bodies and data protection agencies, are essential stakeholders for the HEIR project. These entities are responsible for enforcing regulations and standards related to patient data privacy and cybersecurity in the healthcare sector. HEIR aligns with these regulations, including the General Data Protection Regulation (GDPR) in Europe, and assists healthcare organizations

in meeting compliance requirements. By addressing the concerns of regulatory authorities, HEIR aims to build trust and demonstrate its commitment to safeguarding patient data and upholding regulatory standards in the healthcare domain.

Patients and Patient Advocacy Groups: Patients and patient advocacy groups are increasingly concerned about the privacy and security of their personal health information. They play a significant role as stakeholders in the HEIR project, as the ultimate beneficiaries of robust cybersecurity measures in healthcare organizations. By targeting patients and patient advocacy groups, HEIR aims to instill confidence by offering a cybersecurity platform that protects sensitive patient data, prevents data breaches, and ensures the privacy of medical records. HEIR's focus on threat detection, anomaly detection, and security scoring contributes to maintaining patient trust, which is crucial for the overall success and adoption of the platform.

By considering the perspectives and needs of healthcare executives and administrators, CISOs and IT security professionals, medical and IT staff, regulatory authorities, and patients and patient advocacy groups, the HEIR project can engage key stakeholders and deliver a cybersecurity solution that addresses their specific concerns and priorities. By actively involving these stakeholders, HEIR aims to build strong relationships, foster collaboration, and ensure the successful implementation and adoption of the platform within the healthcare domain.

6. HEIR Competition, SWOT and PEST Analysis

6.1 HEIR Business Competitive Advantage

The HEIR project possesses several key competitive advantages that distinguish it within the healthcare cybersecurity market. These advantages contribute to its ability to effectively address the specific needs and challenges faced by healthcare organizations, ensuring its prominence and success in the industry.

Firstly, HEIR's tailored approach to healthcare cybersecurity sets it apart from generic cybersecurity solutions. By specifically focusing on the unique requirements and regulations of the healthcare domain, HEIR provides a comprehensive platform that aligns with stringent data protection standards. This tailored approach ensures that healthcare organizations can trust HEIR as a specialized solution built to safeguard patient data and meet regulatory compliance.

Secondly, HEIR offers advanced threat detection capabilities that leverage cutting-edge technologies such as Artificial Intelligence (AI) and Machine Learning (ML). These technologies enable the platform to identify and respond to emerging cyber threats in real time. By detecting and mitigating potential risks proactively, HEIR helps healthcare organizations stay one step ahead of cyber-attacks, minimizing the impact on critical systems and patient data.

Another competitive advantage of HEIR lies in its anomaly detection feature. This feature provides healthcare organizations with enhanced visibility into their IT infrastructure, allowing the identification of abnormal patterns or activities that may indicate a cybersecurity breach. By promptly detecting anomalies, HEIR empowers healthcare organizations to respond swiftly and prevent potential data breaches, ensuring the integrity and confidentiality of sensitive patient information.

Additionally, HEIR's security scoring mechanism contributes to its competitive edge. By assessing and assigning a security score to healthcare organizations' cybersecurity posture, HEIR offers a clear metric for evaluating and benchmarking their level of protection. This scoring system not only allows healthcare providers to gauge their own cybersecurity readiness but also provides an objective basis for comparison against industry standards and peers, fostering a continuous improvement mindset and enabling informed decision-making regarding cybersecurity investments and risk mitigation strategies.

Finally, HEIR excels in its visualization techniques and reporting capabilities. The platform offers intuitive and comprehensive visualizations that enable healthcare organizations to gain actionable insights from complex cybersecurity data. Detailed reports provide a holistic view of the organization's security posture, facilitating informed decision-making and efficient allocation of resources. These visualization techniques not only enhance cybersecurity monitoring and incident response but also support effective communication with key stakeholders, including healthcare executives, IT staff, and regulatory authorities.

By leveraging its tailored approach to healthcare cybersecurity, advanced threat detection, anomaly detection, security scoring, and visualization techniques, HEIR establishes a strong competitive advantage within the healthcare cybersecurity market. These advantages enable HEIR to deliver a comprehensive and effective solution that safeguards patient data, protects critical healthcare systems, ensures regulatory compliance, and empowers healthcare organizations to proactively address cyber threats.

6.2 HEIR Competitor Analysis

6.2.1 Threat Detection in Healthcare Cybersecurity

The healthcare cybersecurity market is crowded with many players offering advanced threat detection capabilities. CyberMDX, ClearData, and Fortinet are among the notable competitors of HEIR in this sector.

CyberMDX provides healthcare delivery organizations with an AI-driven cybersecurity solution that proactively identifies, categorizes, and protects connected medical devices from threats. ClearData offers a cloud-based healthcare cybersecurity solution that includes continuous threat monitoring and detection, while Fortinet's healthcare cybersecurity solution includes AI-driven threat intelligence for real-time protection against known and unknown threats.

Despite these competitive offerings, HEIR distinguishes itself with its specific focus on the healthcare sector, leveraging AI and machine learning technologies for advanced, real-time threat detection. The platform's ability to identify and respond to emerging threats provides a competitive edge in the market.

6.2.2 Anomaly Detection

In the area of anomaly detection, Darktrace's AI-driven Cyber AI platform is one of the key competitors. It employs machine learning and AI to detect and respond to anomalous behaviour in real-time, which is especially critical in the healthcare sector due to its sensitivity.

However, HEIR's specific focus on healthcare cybersecurity, coupled with its advanced anomaly detection feature, provides an enhanced level of visibility and insight into the IT infrastructure of healthcare organizations. This empowers these organizations to promptly detect and respond to abnormal activities, effectively mitigating potential cybersecurity breaches.

6.2.3 Privacy-Aware Data Sharing

Privacy-aware data sharing is a critical requirement in healthcare cybersecurity, with competitors like Patientory and MedStack offering specific solutions. Patientory uses blockchain technology to ensure secure and private data sharing among patients, doctors, and healthcare organizations. MedStack delivers a privacy-compliant platform that simplifies the process of building and managing healthcare apps while ensuring data privacy.

HEIR's focus on regulatory compliance and adherence to stringent data protection standards, such as the GDPR, positions it as a reliable solution in the healthcare industry for privacy-aware data sharing.

6.2.4 Cybersecurity Visualization

FireEye's Helix and IBM's QRadar are notable competitors in the cybersecurity visualization sector. FireEye Helix offers a cybersecurity platform with advanced visualization tools, helping organizations understand, prioritize, and manage security events. IBM's QRadar provides a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, and configuration and vulnerability management.

HEIR sets itself apart with superior visualization techniques and detailed reporting capabilities that offer healthcare organizations comprehensive insights into their cybersecurity

posture. This aids in efficient decision-making and effective communication with key stakeholders.

6.2.5 Cybersecurity Scoring

Companies like BitSight and SecurityScorecard are key competitors in the cybersecurity scoring market. BitSight Security Ratings provide a dynamic measurement of an organization's cybersecurity performance, while SecurityScorecard's platform offers security ratings to help organizations manage third-party risk and improve their cybersecurity posture.

HEIR's security scoring mechanism provides a clear and objective metric for evaluating the cybersecurity readiness of healthcare organizations. This helps healthcare organizations benchmark against industry standards and encourages a continuous improvement mindset.

In summary, while there are many players in the healthcare cybersecurity market, HEIR holds a competitive edge with its tailored approach, advanced threat and anomaly detection capabilities, focus on privacy-aware data sharing, superior visualization techniques, and effective cybersecurity scoring systems.

6.2.6 GPU Cluster with SGX Support

In commodity clusters, various companies and organizations offer alternative solutions catering to GPU-accelerated data processing and security. While the proposed module stands out with its unique combination of features, it's essential to understand the strengths and weaknesses of these competitors to position the module in the market effectively.

Competitor 1 – Generic GPU Clusters

Strengths:

- Widely available and offered by multiple vendors, making them accessible to a broad range of users.
- Suited for general-purpose parallel computing tasks, making them versatile for various applications.
- May have lower upfront costs for entry-level setups, appealing to budget-conscious buyers.

Weaknesses:

- Lack the robust security and hardware-based protection provided by Intel SGX technology, which may deter security-conscious customers.
- May not be optimized for industries with strict compliance and data privacy requirements, potentially limiting their adoption in sectors such as healthcare and finance.

Competitor 2 – Cloud-based GPU Services

Strengths:

- On-demand scalability allows users to adjust computing resources as needed, making them flexible for fluctuating workloads.
- Offer a wide range of virtual GPU configurations to cater to different computing requirements, enhancing versatility.
- Integration with other cloud services for data storage and analytics streamlines the workflow and enhances data accessibility.

Weaknesses:

- Data transfer and storage costs can escalate for large-scale computations, potentially leading to unexpected expenses for users with significant data volumes.
- Limited control over the underlying hardware and security measures can be a concern for businesses with stringent security requirements.

Competitor 3 – On-Premises GPU Clusters with Software Security

Strengths:

- Offers better control over hardware and security configurations compared to cloud-based services, appealing to organizations with specific security preferences.
- Can be customized to some extent for specific use cases, allowing for tailored solutions that cater to unique industry demands.
- Suitable for organizations with strict data governance policies, as they maintain data within their premises.

Weaknesses:

- Software-based security measures may not provide the same level of protection as hardware-based solutions like Intel SGX, potentially leaving sensitive data vulnerable to advanced attacks.
- Higher setup and maintenance costs compared to cloud-based solutions can be a deterrent for organizations with budget constraints or limited IT resources.

In a highly competitive market, FORTH's module's unique integration of Intel SGX technology into a commodity cluster of GPUs provides a clear advantage. Hardware-based memory encryption and isolation ensure robust security, setting our solution apart from competitors relying on software-based security measures. This key feature makes our module highly desirable for industries handling sensitive data, including healthcare, finance, and research.

Furthermore, the exceptional performance capabilities of the GPU cluster give it a competitive edge for data-intensive tasks and AI/ML applications, where parallel processing power is critical for efficient computation.

6.2.7 Summary

As seen in Table 3, the HEIR platform, distinguishes itself through tailored threat and anomaly detection, privacy-aware data sharing, superior visualization, and effective security scoring. However, its niche focus might limit applicability beyond healthcare, and initial adoption could be complex. Dependency on data sharing raises concerns, and the GPU cluster's resource intensity may pose challenges. In a competitive landscape, HEIR must address cloud security and evolving regulations while ensuring user adaptation.

Table 3 HEIR Competitor Analysis Aggregated

Component	**HEIR**		**Competitors**	
	Advantage	**Weakness**	**Advantage**	**Weakness**
Threat Detection in Healthcare Cybersecurity	Advanced threat detection focused on healthcare, leveraging AI and machine learning for real-time insights.	HEIR's healthcare-specific focus might limit its versatility beyond the healthcare sector	**CyberMDX, ClearData, Fortinet**	
			AI-driven cybersecurity solutions for connected medical devices; real-time threat monitoring	Less specific to healthcare, broader focus
Anomaly	Specific healthcare	Initial	**Darktrace**	

Detection	anomaly detection for swift identification and response	complexity, potentially leading to resistance during initial adoption	AI-based real-time anomaly detection	Generalized application, less tailored to healthcare
Privacy-Aware Data Sharing	Strong focus on regulatory compliance, ensuring trustworthy healthcare data sharing	HEIR's efficacy hinges on healthcare institutions sharing data, potentially raising concerns about data privacy and ownership	**Patientory, MedStack**	
			Blockchain-based secure data sharing	Potential limitations in scalability or complexity
Cybersecurity Visualization	Detailed reporting and superior visualization for comprehensive insights	HEIR's challenge lies in a competitive market with HEIR's focus only on healthcare-specific insights	**FireEye's Helix, IBM's QRadar**	
			Advanced visualization tools	Focus on broader security landscape, not healthcare-specific
Cybersecurity Scoring	Clear security scoring mechanism promoting continuous improvement	HEIR's Observatory reliance on cloud services could pose security concerns	**BitSight, SecurityScorecard**	
			Security ratings aiding risk management	May lack healthcare-specific metrics
GPU Cluster with SGX Support	Hardware-based security and exceptional performance	Resource-intensive setup and maintenance	**On-Premises GPU Clusters with Software Security**	
			Control over hardware and security	Software-based security might be less robust

6.3 PEST Analysis

PEST analysis is a strategic framework used to analyze the external factors that can impact the success and performance of an organization or a specific project. PEST stands for Political, Economic, Social, and Technological factors. In the context of the HEIR project, conducting a PEST analysis becomes essential to comprehensively assess the external factors that may influence the success and adoption of the cybersecurity platform tailored for the healthcare domain. HEIR, an innovative solution offering threat detection, anomaly detection, security scoring, and visualization techniques, operates within a dynamic environment shaped by Political, Economic, Social, and Technological factors. By conducting a PEST analysis, the HEIR project can gain valuable insights into the political landscape, including healthcare regulations and government support for cybersecurity initiatives. The PEST analysis can

provide valuable insights to the HEIR project, enabling strategic decision-making to leverage opportunities and address challenges in the ever-evolving healthcare cybersecurity landscape.

Political Factors

Government Regulations: The healthcare industry operates under strict regulatory frameworks to protect patient privacy and data security. HEIR complies with laws such as the General Data Protection Regulation (GDPR) in Europe. Adhering to these regulations ensures that healthcare organizations using HEIR remain compliant and avoid legal penalties.

Government Support: Governments are increasingly recognizing the importance of cybersecurity in healthcare. They provide support through funding initiatives, cybersecurity guidelines, and collaborations to enhance the adoption and effectiveness of platforms like HEIR. Leveraging government support can help HEIR gain market traction and establish credibility.

International Collaboration: HEIR can leverage the potential for international collaboration in addressing healthcare cybersecurity. Collaborative efforts between governments and cybersecurity organizations can facilitate knowledge sharing, standardization of cybersecurity practices, and coordinated responses to global cyber threats, creating a conducive environment for the adoption and growth of HEIR in different regions.

Cybersecurity Legislation: Governments are enacting or updating cybersecurity legislation to combat emerging threats. HEIR should closely monitor legislative developments and ensure that its platform aligns with the evolving regulatory requirements. By staying compliant and keeping abreast of changes in cybersecurity laws, HEIR can position itself as a trusted solution that helps healthcare organizations meet their legal obligations.

Economic Factors

Cost Efficiency: Healthcare organizations often face budget constraints. HEIR can provide cost-effective solutions that offer high-value protection against cyber threats. The platform's pricing model should align with the financial capabilities of healthcare providers, ensuring affordability and return on investment.

Economic Impact of Cyber Attacks: The financial repercussions of cyber-attacks in healthcare can be severe, including data breaches, legal penalties, reputational damage, and operational disruptions. HEIR can position itself as a crucial investment for healthcare organizations, emphasizing the potential cost savings and mitigating financial risks associated with cyber threats.

Return on Investment (ROI): HEIR should highlight the potential ROI healthcare organizations can achieve by implementing the platform. This includes cost savings associated with preventing data breaches, minimizing operational disruptions, and avoiding legal penalties. Demonstrating a positive ROI will incentivize healthcare providers to invest in HEIR as a strategic cybersecurity solution.

Market Growth and Opportunity: The healthcare cybersecurity market is experiencing rapid growth due to increasing cyber threats. HEIR should leverage this growth to expand its market presence. By identifying emerging markets and strategic partnerships, HEIR can seize new opportunities and secure a competitive advantage, driving further revenue growth.

Social Factors

Awareness and Perception: Public awareness regarding cybersecurity risks in healthcare is increasing. HEIR can capitalize on this by promoting its advanced threat detection, anomaly detection, and security score capabilities as key differentiators. By effectively communicating

the importance of protecting patient data and maintaining trust, HEIR can foster a positive perception among healthcare providers and patients.

Employee Training and User Experience: HEIR should prioritize user-friendly interfaces and comprehensive training programs to ensure ease of use and adoption. Empowering healthcare professionals with the necessary skills and knowledge to navigate the platform efficiently will contribute to a culture of cybersecurity awareness and proactive threat mitigation.

Trust and Reputation: Trust is a crucial factor in healthcare. HEIR should emphasize its ability to safeguard patient data, protect critical healthcare systems, and maintain the trust and reputation of healthcare organizations. Positive user testimonials, case studies, and certifications can enhance HEIR's reputation, fostering trust among healthcare professionals, patients, and stakeholders.

Public Perception of Privacy: Heightened public awareness of data privacy issues has raised concerns about the security of personal health information. HEIR should position itself as a privacy-focused cybersecurity platform, implementing strong data encryption, access controls, and other privacy-enhancing measures. Demonstrating a commitment to protecting patient privacy can build a positive perception and increase adoption of HEIR.

Technological Factors

Advancements in Threat Detection: HEIR must stay ahead of evolving cyber threats in the healthcare domain. Incorporating cutting-edge technologies such as artificial intelligence (AI), machine learning (ML), and behavioral analytics into its threat detection and anomaly detection capabilities can enhance its effectiveness in identifying and mitigating emerging threats.

Visualization Techniques: HEIR's visualization techniques should provide intuitive and actionable insights for healthcare professionals. User-friendly dashboards, real-time analytics, and comprehensive reporting features will enable healthcare organizations to gain a holistic view of their cybersecurity posture and make informed decisions to enhance their security measures.

By considering these political, economic, social, and technological factors, HEIR can effectively position itself as a robust cybersecurity platform tailored for the healthcare domain, catering to the unique needs and challenges of healthcare organizations while addressing regulatory compliance, financial constraints, user experience, and technological advancements.

Internet of Medical Things (IoMT): The proliferation of connected medical devices increases the attack surface for cyber threats. HEIR should adapt its threat detection capabilities to address the unique challenges posed by the IoMT. By monitoring and securing the network of interconnected devices, HEIR can help healthcare organizations mitigate risks associated with vulnerable endpoints.

Cloud Adoption: The healthcare industry is increasingly adopting cloud-based solutions. HEIR should align its platform with cloud infrastructure and provide seamless integration with popular cloud service providers. Offering secure cloud deployment options and ensuring data protection during storage and transmission will cater to the evolving needs of healthcare organizations embracing cloud technologies.

6.4 SWOT Analysis

This section will only present the updates in the SWOT Analysis gained during the progress of the HEIR project after the submission of deliverable D7.7.

Strengths:

Tailored Approach: HEIR is a platform specifically built to cater to the needs of healthcare institutions, providing customized cybersecurity solutions, unlike generic cybersecurity products.

Holistic Solution: The HEIR platform integrates a broad variety of cybersecurity solutions, tackling a wide spectrum of critical aspects of cybersecurity in healthcare institutions.

Technological Edge: HEIR leverages advanced technologies such as AI and machine learning for advanced threat detection and anomaly detection.

Compliance Focus: The platform aligns with stringent data protection standards like the GDPR, ensuring compliance for healthcare organizations.

Unique Value Proposition: HEIR's unified framework provides a holistic approach to cybersecurity in the healthcare domain and promotes awareness among all stakeholders.

Weaknesses:

Market Competition: The cybersecurity market is crowded with many players, and distinguishing HEIR's offering can be challenging.

Adoption Hurdles: Cybersecurity measures can often be perceived as complex and challenging to implement, creating potential adoption hurdles.

Resource Requirements: Ensuring continuous updates and maintenance of the HEIR platform to keep up with the evolving threat landscape can require significant resources.

Opportunities:

Increasing Cyber Threats: With the increasing digitalization of healthcare data and rising cyber threats, there is a growing demand for effective cybersecurity solutions in the healthcare sector.

Regulatory Environment: The increasing focus on data privacy regulations presents an opportunity for platforms like HEIR that adhere to such stringent standards.

Growing IoMT Market: The expanding Internet of Medical Things (IoMT) market requires robust cybersecurity measures, providing significant opportunities for HEIR.

Threats:

Rapid Technological Changes: The rapid evolution of technology and the cybersecurity landscape requires HEIR to continuously update its platform to stay effective.

Sophisticated Cyber Attacks: The increasing sophistication of cyber threats may challenge the HEIR platform's ability to effectively counter them.

Regulatory Changes: Changes in regulatory norms related to data privacy could pose challenges and require the platform to adapt quickly.

The HEIR project should capitalize on its strengths and opportunities, address its weaknesses, and have a strategy to mitigate potential threats. The project's unique selling points should be highlighted in its market positioning and exploitation plans.

STRENGTHS	WEAKNESSES
Tailored Approach for the Healthcare Cybersecurity domain **Holistic Solution** **Technological Edge** **Compliance Focus** **Promotes healthcare cybersecurity awareness at EU level**	**Crowded Market** **Adoption Hurdles** **Resource Requirements**

OPPORTUNITIES	THREATS
Increasing Cyber Threats **Regulatory Environment** **Growing IoMT Market**	**Rapid Technological Changes** **Sophisticated Cyber Attacks** **Regulatory Changes**

Figure 17 SWOT Analysis

7. HEIR Intellectual Property Rights

In this section, we will provide an overview of several key tools developed for the HEIR project and their respective IPR information. More specifically, we will discuss the licensing and exploitation strategies, pricing models, and target markets, to offer a complete understanding of each tool's functionalities and commercial potentials.

7.1 The HEIR Platform

The HEIR platform integrates different tools, each with distinct IPR guidelines. AEGIS's Forensics Visualization Toolkit will be offered under a proprietary license, while its visual interfaces span both free LGPL on-premises installations and a proprietary SaaS model. IBM's Privacy-Aware Framework, based on the Fybrik Open-Source structure, is accessible under the Apache 2.0 license. The Observatory tool by AEGIS is going to adopt an LGPL licensing scheme, whereas ITML's SIEM System blends open-source elements with proprietary methodologies for a SaaS offering. The specific IPR information for each tool of the HEIR platform will be described in more detail in the following subsections.

7.2 HEIR's Forensics Visualization Toolkit

Developed by AEGIS, the FVT is an advanced visualization toolkit that has a broad application scope, including digital forensic analysis and big data analytics. Its data protection layer decouples the data processing logic from various controls, including access, privacy, and governance. The toolkit will be available under a proprietary AEGIS license beyond the HEIR project's completion. Pricing is dependent on the scale of the customer's needs, taking into account factors such as the number of endpoint devices to monitor and the number of users accessing the toolkit.

7.3 HEIR's Visualizations

These interfaces, designed by AEGIS, will be available under two different formats: a) a customer on-premises installation available for free to primary markets under LGPL license, and b) as a SaaS, where AEGIS maintains the hosting of the GUI, under a proprietary license. Pricing details have not been defined yet, but they will depend on the number of users accessing the GUI.

7.4 HEIR's Privacy-Aware Framework

IBM's Privacy-Aware Framework uses the Fybrik Open Source framework to provide a flexible and powerful solution for policy-driven data compliance. It allows fine-grained access to data without requiring modifications to backend storage systems. This tool, licensed under Apache 2.0, is suitable for any market segment that needs to protect sensitive or personal data.

7.5 HEIR's Observatory

The Observatory tool, owned by AEGIS, leverages the Advanced Visualization Toolkit to cater to the needs of policymakers and regulators. This tool integrates contributions from multiple parties including Bitdefender, Sphynx, and ITML. Licensing is expected to be under a common scheme such as LGPL. Its exploitation strategy includes targeting both the public and private healthcare sectors, with a provision for the Observatory as a service.

7.6 HEIR's SIEM System

Developed by ITML based on their expertise in cybersecurity, the HEIR SIEM tool provides real-time threat monitoring and cyberattack management. Though built using open-source components, its internal methodology remains proprietary. The tool will be offered as a SaaS under a service license with pricing based on usage or a flat rate.

7.7 HEIR's Aggregator

The HEIR Aggregator is a connecting tool within the HEIR platform. It collects and aggregates data generated by HEIR clients and the RAMA calculator, orchestrating their transmission to HEIR's 1st Layer GUI and the Observatory. It was developed by SIEMENS SRL and will be made available under a proprietary license after the end of the HEIR project.

7.8 HEIR's Local and Global RAMA score

The Local and Global RAMA Calculator by STS is a risk assessment tool developed from STS. The Local and Global RAMA score algorithms will be publicly available, while the methodology and the calculator's implementation will not be open-sourced. Healthcare organizations are the main target for the Local RAMA score, which will be offered under a license agreement with the HEIR client.

7.9 Security and Privacy Assurance (SPA) Suite

SPHYNX's Security and Privacy Assurance Suite provides a holistic risk assessment platform. The offerings of this suite are proprietary. The tool will be offered as a SaaS or PaaS under a service license with pricing based on usage or a flat rate.

7.10 HEIR's Client

The HEIR Client, developed and owned by Bitdefender, includes various modules for network monitoring, threat detection, and risk assessment. The target market for the HEIR Client is the global cybersecurity market for healthcare, which is estimated to reach $57.25 billion by 2030.

7.11 Anomaly Detection

Developed by TUD, the Anomaly Detection (AD) tool redefines real-time anomaly detection and threat classification. Adapting supervised and unsupervised models aligns with cyber security rules and threat levels. It assimilates existing ML models tailored for health systems' needs, effectively categorizing event and threat data. Operating on HEIR's IoT logs, the ML module extracts anomalies and then compiles detailed reports. Insights materialize through the FVT toolkit. Tailored models for distinct use cases (PAGNI, CROYDON) underscore its adaptability. This TUD innovation evolves anomaly detection into a Software-as-a-service solution.

7.12 GPU Cluster with SGX Support

FORTH has customized the GPU cluster to fit the needs of research and healthcare infrastructures. FORTH's cluster will be available under a proprietary license beyond the end of the HEIR project.

7.13 IPR Status Summary

The table below provides an organized overview of various IPRs associated with tools used in the HEIR project. It summarizes key information such as the tools' names, IPR background

and foreground, ownership details, license types, applications in the project, and their respective exploitation and commercialization strategies.

Table 4 HEIR's IPRs

Tool	IPR Background	IPR Foreground	Owner	License	Exploitation / Commercialization
HEIR's Forensics Visualization Toolkit	AEGIS's extensible software ranging from Digital Forensic Analysis to Big Data analytics	Framework adding data protection layer decoupling data processing logic from data access, control, governance, etc	AEGIS	Proprietary AEGIS license	Scale-based pricing package
HEIR's Visualizations - Customer On-premises installation	-	-	AEGIS	Free under LGPL; Full version under proprietary license	Pricing not defined yet; package based on number of users
HEIR's Visualization - SaaS	-	-	AEGIS	Proprietary license	Pricing not defined yet; package based on number of users, with a maximum trial period of 6 months
HEIR's Observatory	AEGIS's extensible software; Intellectual Property of Bitdefender, Sphynx, ITML	Customized AEGIS Advanced Visualization Toolkit; threat hunting module by ITML; security assurance platform by Sphynx; "collaborative privacy-aware framework" tool by IBM	AEGIS	Proprietary license; Common and sustainable license scheme (e.g., LGPL)	Subscription service; Two-sided business model of a marketplace considered
HEIR's SIEM system	ITML's Security	Tool for real-time threat	ITML	Service (SaaS)	Software-as-a-Service (SaaS)

	Infusion for real-time threat monitoring and cyberattack management	monitoring developed in the context of ITML's "Security Infusion" commercial product		license	model
HEIR's Aggregator	-	-	SIEMENS	Proprietary license;	License agreement; SaaS
HEIR's Local and Global RAMA score	STS's SPA suite including various risk assessment methods	Local RAMA score algorithms, methodology, and implementation	STS	-	License agreement; through publications; through standardisation of output format; through contract research
Security and Privacy Assurance (SPA) Suite	STS' SPA Suite	-	STS	-	SaaS or PaaS model
HEIR Client	Technologies developed by Bitdefender before and during the project	-	BD	-	Targeted at the global cyber security market for healthcare
HEIR's Privacy-Aware Framework	Fybrik Open Source framework from IBM	Implementations of Privacy Aware Framework created as foreground	IBM	Apache 2.0	Any market segment that needs to protect access to sensitive/personal data
GPU Cluster with SGX Support	-	Development of a GPU cluster with Intel SGX support	FORTH	Proprietary license	Software-as-a-Service (SaaS) model
Anomaly Detection	TUD's Machine Learning component facilitates intelligent anomaly detection and threat	Development of both supervised and unsupervised models in order to capture the anomalies.	TUD	-	Software-as-a-Service (SaaS) model

	classification				

8. Conclusion

HEIR is trying to tackle the one of the most important issues of today's world: cybersecurity in the healthcare domain. To enhance the security of healthcare environments and mitigate risks, there is a demand for a comprehensive end-to-end cybersecurity approach. HEIR offers a holistic cyber-intelligence platform for healthcare environments, facilitating secure data exchange across healthcare and research organizations with high levels of resilience, reliability, accountability, and trustworthiness. The platform addresses threat prevention, detection, mitigation, and real-time response.

The market analysis reveals promising prospects for HEIR. The healthcare security market is expected to experience a significant compound annual growth rate (CAGR) of over 14 to 16%[35,36].

This presents an opportune moment for HEIR to capitalize on key challenges and market drivers, adopting a customer-centric value approach and establishing capabilities to support business modelling for each market. Despite tough competition, HEIR distinguishes itself technologically as a platform supporting multi-level security in healthcare environments, encompassing different technologies to build the Risk Assessment for Medical Applications (RAMA). It boasts multiple novel components, employing highly innovative approaches to address several security requirements specific to industrial environments facing the complex challenges of the healthcare domain.

HEIR also holds a unique business advantage compared to existing solutions. It offers a granular approach and caters to various security requirements at all levels, enabling potential users to selectively choose and pay only for the novel components they need from a vast list of HEIR components. This flexibility allows for tailored solutions that precisely address the specific needs of involved industrial sites.

[35] https://www.marketsandmarkets.com/Market-Reports/healthcare-cybersecurity-market-215097518.html
[36] https://www.grandviewresearch.com/industry-analysis/healthcare-cyber-security-market

9. References

Accenture. (2021). *Cybersecurity: A Critical Business Issue for the Board.* Accenture.

T. C. Truong, I. Z. (2020). Artificial Intelligence and Cybersecurity: Past, Presence, and Future. *Dash, S., Lakshmi, C., Das, S., Panigrahi, B. (eds) Artificial Intelligence and Evolutionary Computations in Engineering Systems. Advances in Intelligent Systems and Computing.* Springer.

Victor R. Kebande, N. M. (2021). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*, 5–17.