



REWIRE - Cybersecurity Skills Alliance A New Vision for Europe

R.5.1.1 CyberABILITY Platform



Title	R5.1.1 CyberABILITY				
Document description	The present deliverable serves as a short description of the CyberABILITY platform. This deliverable is complementary to T5.1 whose main output is the platform.				
Nature	Public				
Task	T.5.1 Design and Development of the Digital European Cybersecurity Skills Observatory				
Status	Draft				
WP	WP5				
Lead Partner	TUC				
Partners Involved	All				
Date	06/03/2024				

Disclaimer:

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use that may be made of the information contained therein.

PUBLIC

Contents

Executive	e Summary	4
1. REWIR	E Cyberability platform	4
1.1. Tech	nology Stack	4
1.1.1.	Back-end	4
1.1.2.	Front-end	4
1.1.3.	Version Control	5
1.2. Com	ponents	5
1.2.1.	Cybersecurity Job Ads Analyzer	5
1.2.2.	Cyber Security Profiler	10
1.2.3.	ECSF Explorer	13
1.2.4.	Career Path / Development	14
1.3. Acce	ess and documentation	18



EXECUTIVE SUMMARY

The CyberABILITY platform emerges as a publicly available, digital online hub, designed to bridge the existing gap in the cybersecurity domain across Europe. It is a publicly accessible platform that provides insights into the job market, competencies, training courses, and certification schemes. This platform not only serves as a bridge between demand, abilities, and training resources but also fosters knowledge sharing and intra-institution collaboration, thereby significantly enhancing the cybersecurity skill set across the continent.

Through regular updates in the last year of the REWIRE project, the CyberABILITY platform will substantially address the cybersecurity skills gap, making it an asset in the evolving cybersecurity landscape.

1. REWIRE CYBERABILITY PLATFORM

1.1. Technology Stack

1.1.1. Back-end

CyberABILITY's backend infrastructure is built upon the robust combination of PHP and MySQL, ensuring a seamless and efficient data management system. PHP, known for its server-side scripting capabilities, facilitates dynamic content delivery, while MySQL, a renowned relational database management system, ensures data integrity and swift retrieval. Together, they form the backbone of the CyberABILITY platform, providing a stable, scalable, and secure environment that can handle vast amounts of data and user interactions, ensuring optimal performance and reliability for its users.

In particular, the server part of the application consists of several PHP (i.e., PHP: Hypertext Preprocessor) scripts, located on the web server next to the source JavaScript codes of the client part. These server scripts handle requests coming from clients' Internet browsers and serve as an intermediary for data manipulation. Each script is for a specific action. They are triggered by a query for a specific URL such as *https://SERVER_URL/addJob.php*. The scripts require specific data in the query body according to the required operation, as well as an authorization token. They will read or write data to the application database based on a valid request. The connection to the database is provided by PHP Data Objects (PDO), which helps to prevent SQL injection and character set inconsistencies by design.

1.1.2. Front-end

CyberABILITY's frontend is developed using ReactJS, a JavaScript library known for its efficiency in building interactive user interfaces. Specifically, the platform leverages the Antd package, a high-quality React component library that offers a suite of rich UI elements and

widgets. This combination ensures that CyberABILITY's frontend is not only responsive and user-friendly but also aesthetically pleasing, adhering to modern design principles.

1.1.3. Version Control

Git is used as a version control system, ensuring a streamlined and efficient development process. Using git, developers from BUT and TUC who are the technical partners involved in the development process, can track modifications, collaborate seamlessly across different features, and maintain a comprehensive history of code changes. This adoption not only safeguards the integrity of the platform's codebase but also facilitates agile development, allowing for rapid iterations and adjustments.

1.2. Components 1.2.1. Cybersecurity Job Ads Analyzer

Cybersecurity Job Ads Analyzer is a dynamic web application to identify which cybersecurity skills are required in a work role. The tool has four main views: **1**) **The database**, **2**) **The Machine Learning (ML) results**, **3**) **Create your ad** tab, and **4**) **The statistics** tab. The **database** allows users to add job adverts and filter the adverts using several fields such as country and year. When this deliverable was submitted, the Job Ads Analyzer counted 938 jobs inserted thanks to the joint effort of the whole REWIRE consortium. The database is depicted in Figure 2. The application database is implemented on the same machine via the MySQL server MariaDB. The database currently contains only a table with users and a table with job adverts. The job table contains, in addition to the values displayed on the web, dozens of other parameters that act as raw truths for the ML algorithm. For a better visualization, a map showing the number of job ads per country has been developed as shown in Figure 1. In the map, job adverts are split per country and several filter options are also available.





AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B



Figure 1 - The map

Furthermore, Job ads can easily be added through the application, as shown in Figure 2, after creating an account in the platform.





the job ad	
General	Cybersecurity Skills Other IT Skills Soft Skills
* Title	Senior Information Security Analyst
Source	LinkedIn
* Link	https://www.linkedin.com/jobs/view/2487448959/?alternateChannel=searcl
* Company	Conduent
* Country	Czech Republic \lor
Continent	Europe
* Date	2021-01-01
ENISA Profile	Cybersecurity Risk Manager \vee
Secondary ENISA Profile	Cybersecurity Auditor
Partners	UT
* Description	What is Job about? The Senior Information Security Services Analyst is the local security professional assigned to a Conduent Business Unit(s), Site or Strategic function / initiative. The Senior Information Security Services Analyst is responsible for ensuring good security risk management
Filename	CZ_20210420_Senior.txt
	Generated automatically
Comment	0
Updated	2023-07-12 09:27:53
Created	2021-11-04 19:16:59

Figure 2 - The Add Job tab

ML results show the identified cybersecurity skills within the selected job adverts. The analysis of skills needs in the market started to be developed in WP2 and fed in WP3. This tool supports the achieved results. We refer to R3.6.1 European Cybersecurity Blueprint for more details. The ML algorithm for skill prediction and keyword processing is implemented as a Python program. The program consists of a tokenizer and an LSTM model. The machine learning model can also be re-created and re-learned. The ML program is stored on the webserver in a sub-directory of web content. When requesting data processing by the ML algorithm, an HTTP request is sent from the client application to a PHP script which, in the first step, reads all the necessary data from the database and creates a dataset in a temporary directory on the server. In the second step, the PHP script executes the terminal command using *exec* function to run the Python ML program. After performing the ML analysis, the program outputs the return code back to the PHP script and creates the analysis output files

PUBLIC

in a temporary folder. The PHP script then loads these files, processes them, and sends the results back to the client application for viewing by the user. This tool has already been extended to adopt the ENISA framework. A new field "Profile" allows assigning the ENISA profile to the job ads. Therefore, by selecting the job ads related to a profile one can compare the skills assigned to it in the framework to the ones suggested by the labor market. The database with the possibility to select ads related to a specific ENISA profile is shown in Figure 3.

REWIRE 🏠 Home Job Ads Analyzer …				8 Lo
	Cybersecurity Job Ads Analyzer			
+ Add job Clear filters and sorters Clear selection				Show in map
] Y Title		0 T Country	⊕	Partners 🗘
Senior Information Security Analyst	LinkedIn Conduent	Czech Republic		UT
Information Technology Security Manager	LinkedIn Global Blue	Austria		UT
Security Analyst	LinkedIn Oracle	Czech Republic	Chief Information Security Officer Cyber Incident Responder	BUT
Infrastructure Security Architect - Prague	① LinkedIn AVON	Czech Republic		BUT
Tier 1 Security Engineer	① LinkedIn Verizon	Czech Republic	Cyber Legal, Policy & Compliance Officer	BUT
CYBER SECURITY & IT COMPLIANCE MANAGER (M/F)	① LinkedIn Rieter	Czech Republic	Cybersecurity Architect	BUT
Group Product Manager	Uinkedin Avast	Czech Republic	Cybersecurity Auditor	BUT
Threat Hunting & Response Senior Analyst	LinkedIn Novartis Czech Republic	Czech Republic	Cybersecurity Educator	BUT
Associate Security Engineer	LinkedIn Blackboard	Czech Republic	Reset OK	BUT
Security Engineer	Ulinkedin CGI Space	Czech Republic	Europe 2021 CAu	BUT
			Selected 0 items	Process
				10 /

Figure 3 - The database

The **create your ad** environment supports the design of a new ad with the analysis of the provided text. A user can use the ML algorithm to check which skills are in its description and compare them with the ones normally proposed in similar job ads through the ENISA characterization. Figure 4 shows the analysis of a description meant for a cybersecurity architect with identified skills and match to ENISA profiles. By pointing on the coverage of a profile, a list of suggested skills is provided.



Create Your Own Ad

Fill in a description of your job and analyze it.

Design, implement and govern of security architectures and supporting processes, perform required information security analyses (including: risk assessment), support in data collection and analysis of cybersecurity-oriented process, have strong problem-solving skills, solid know-how about information security management frameworks (e.g. ISO 27000, NIST CSF), excellent communication skills with the ability to work effectively with a diverse range of stakeholders, security analysis of infrastructure architect Analyze Search BIAS List of Found Skills Skill Collaborate and Communicate Data Analysis Data Privacy Data Security Enterprise Architecture and Infrastructure Design Information Security Controls Assessment Information Systems and Network Security Intelligence Analysis Operating Systems Problem solving and Critical Thinking Project Management

Risk Management System Administration Included Skills Testing and Evaluation · Collaborate and Communicate Threat Analysis Data Privacy Data Security Enterprise Architecture and Infrastructure Design List of Enisa Profiles · Information Systems and Network Security Risk Management Profile **Missing Skills** Chief Information Security Officer (Ciso) Software Development Cyber Incident Responder Technology Fluency Workforce Management Cyber Legal, Policy & Compliance Officer Cyber Threat Intelligence Specialist Cybersecurity Architect 67 % Cybersecurity Auditor 25% Cybersecurity Educator 25 %

88 % Cybersecurity Implementer Cybersecurity Researcher 56 % Cybersecurity Risk Manager 57 % Digital Forensics Investigator 67 % Penetration Tester 50 %

Figure 4 - Create your ad tab

Moreover, a gender balance analysis can be run on the text and, in case the text is found gender-oriented, an alternative text is provided with the help of a ChatGPT model. This analysis can be applied by pushing on the button BIAS.

REWIRE



AGREEMENT NO.

9

Finally, the **statistic** tab shows the ML results on the whole dataset, i.e., the top 10 skills identified and the radar plot of the skills occurrences. Figure 5 depicts the results.

		List of the 10 most sought-at	fter skills (for medium dataset)	
	Rank	Skill		Occurrence
	1	Collaborate and Communicate		85.28 %
	2	Information Systems and Network Security		67.41 %
	3	Information Security Controls Assessment		65.05 %
	4	Business Continuity		50.2 %
	5	Risk Management		49.41 %
	6	Threat Analysis		48.75 %
	7	Organizational Awareness		48.62 %
	8	Incident Management		46.65 %
	9	Data Security		45.07 %
	10	Enterprise Architecture and Infrastructure Design		44.55 %
k	Asset dentity Mana	additional metallicity and the second	CO CO CO CO CO CO CO CO CO CO CO CO CO C	gement ganizational Assumess
Dig	gital Forensic		200	Threat Analysis
Education and Trainin	ig Delivery		100	Incident Management
Data	a Analysis		•	Data Security
Software D	evelopment			Enterprise Architecture and Infrastructure Design
Netwo	ork Manager	tent		Project Management
	System Ac	ministration	Strate	gic Relationship Management
		Technology Fluency	Policy Developm	tenî.
		Law, Policy, and Ethics	Testing and Evaluation	
		Operating Systems	Intelligence Analysis	
		Workforce Management	Problem solving and Critical Thinking	

Statistics

Figure 5 - Statistics tab

1.2.2. Cyber Security Profiler

The Cyber Security Profiler has been created to collect and analyze cybersecurity skills in curricula, trainings, and certification schemes. Moreover, this app helps to create a bridge between demand and offer in cybersecurity with a clear career path starting from the studied skills to the work roles that can be achieved. Filtering features and statistics are shown as well as the possibility to create your curricula, certification, or training while having on-time statistics and connection to the ENISA profile and NICE work roles.

The Cyber Security Profiler (CSP) is built on Cybersecurity Curricula Designer (CCD-v2) and will extend it with additional features. It must be emphasized that the CCD is a result of SPARTA, while CSP will be a result of REWIRE. The main differences are:

1. The CSP app will extend the CCD-v2 by cybersecurity trainings and certifications. helps users to create new or upload existing trainings or certifications in compliance with ENISA requirements.

2. Furthermore, the CSP app allows uploading/creating databases of existing curricula, trainings, and certifications with bilateral flow

For more information we refer to R3.4.1 Mapping the framework to existing courses and Schemes.

The tool has three main views: 1) Curricula, 2) Training, and 3) Certification.

These environments have similar features, for instance, in curricula a user can create courses, drag them in the central column and several statistics will be displayed. Figure 6 sketches an example of curricula courses and statistics.

Cyber Security Profiler Home M							(Log In
Available Courses			Your C	Your Curricula		Statistics		
Add course S	ample courses loaded		Import	Export		Total ECTS credits:		
Mandato	ry Courses		1st	vear		winter	summer	sum
mandato	iy ooulooo		100	year	1st year	6	11	17
winter semester	summer semester		winter semester	summer semester	2nd year	0	6	6
winter mandatory course 🛛 🗖	summer mandatory course	/ 0	winter mandatory course 🛛 🖈 🗙	summer mandatory course 🖉 🗶	3rd year	0	0	0
Computers and Programming 1 Computer Science - Computer Systems	Incidents Security		Communication Technologies Computer Science / Security - Computer Networks	Computers and Programming 2 Computer Science - Software Engineering	sum			23
Software Engineering		_	Network Security		NIST NICE Framework	ECSF Framew	ork Beta	
Winter mandatory course Foundations of Cryptography Cryptology - Fundamental Cryptology	summer mandatory course Mathematics Mathematics • Topology and Analysis	/ 0		summer mandatory course X X Data Communication Computer Science - Communication Theory		ECTS by SPART	TA areas:	
winter mandatory course CE Legal Theory Humanistic & Social Sc. • Law and Regulations	summer mandatory course Physics Privacy - Data Extraction	~ 0	2nd winter semester	year summer semester				
writter mandatory course Adathematics 1 Mathematics Algebra and Discrete Mathematics Topology and Analysis	summer mandatory course Theoretical Informatics Computer Science • Theoretical Computer Science	/8	Drep Course Here	summer mandatory course XX Discrete Mathematics Mathematics - Algebra and Discrete Mathematics - Number Theory	Comp Mathema	13% uter Science Cry tics Privacy O Other	26% ptology O Security Humanistic & Social Sc.	
winter mandatory course Multimedia Services Computer Science / Security Computer Science / Security			3rd	year		ECTS by SPART	A topics:	
Network Security			winter semester	summer semester	Topic			ECTS
uiteter mandatore opures					Communication Theory			26.1%
Privacy					Computer Networks			13%
Privacy / Humanistic & Social Sc.			+	-	software Engineering			21.7%

Figure 6 - Curricula tab

Moreover, a user can export and then import its work any time. This tool is also a database, therefore, a user can either create and analyse a created curriculum, training, or certification scheme or brose in the dataset. Figure 7 shows a filtering of the available trainings. The training information are provided such as language, description, and skill coverage. Once the trainings are selected, they can be loaded and analyzed in a similar environment as in Figure 6 for curricula.

Browse available trainings							
∓ Filter by	Trainings 36/64						
I heoretical and hands on Theoretical only Duration	Cyber Systems Security through Ethical Hacking I	Cyber-Security for protection of classified information I					
10 1152 12 16 180	Cyber Systems Security through Ethical Hacking II	Overview Details Description Loorn why other accurity is important in the process of protection of					
Language	Cyber-Security for protection of classified information I	classified information and how to protect classified information from the perspective of INFOSEC (security of electronic classified information)					
Czech Dutch Finglish French	Hacking: Binary Exploitation	Powire skill groups					
Mare 🗸 Skills group	CyberHOT Summer School II	Data Security incident Management					
Business Continuity Collaborate and Communicate Data Analysis Data Privacy	Cyber Security in e-Governance						
Data Security More V	Cyber Security for Blockchain						
Timing Available online Fixed dates	CyberSecurity Essentials						
On demand	Technical Basics and						
		1 trainings selected Close Load					
	Eiguro 7 Brows	available trainas tab					

Figure 7 - Browse available traings tab

The CS Profiler app among other trainings, also interfaces the "CONCORDIA interactive map of trainings"¹. One can explore the trainings and have a detailed overview of the percentage-based profile matching.

In the picture below, the "Cyber Incident Handling Workshop" offered by Airbus Cybersecurity and also present in the CONCORDIA map, is analyzed.



PUBLIC¹ <u>https://www.concordia-h2020.eu/map-courses-cyber-professionals/</u>

Your Trainings	Statistics	
Import Export	ENISA Profiles coverage:	
	Profile Name	Coverage
ining 🖍 🗙	Chief Information Security Officer (Ciso)	23 %
Cyber Incident Handling	Cyber Incident Responder	25 %
orksnop	Cyber Legal, Policy & Compliance Officer	20 %
s cybersecurity Germany	Cyber Threat Intelligence Specialist	10 %
	Cybersecurity Architect	22 %
	Cybersecurity Auditor	0 %
	Cybersecurity Educator	25 %
	Cybersecurity Implementer	13 %
	Cybersecurity Researcher	11 %
	Cybersecurity Risk Manager	14 %
	Digital Forensics Investigator	17 %
	Penetration Tester	17 %
	Result (median)	17 %

Figure 8 - Example ECSF Profile Training Coverage

1.2.3. ECSF Explorer

The ECSF Explorer is a tool that enables users to explore the ECSF (European Cybersecurity Skills Framework)² interactively. Figure 7 shows its main view. By clicking on the roles, users can view alternative titles, summary statements, missions, deliverables, main tasks, key skills, key knowledge, and e-competences. Within the e-competences section, hovering over the level tags reveals their descriptions.

The primary objective of this application is to provide a more efficient and user-friendly alternative to the traditional method of manually searching through the document. Instead of spending valuable time and effort scrolling through pages and trying to locate specific information, users can now leverage this web-based tool. By transitioning to this application, users can not only save time but also enhance their overall experience.

Following similar styling and layout, depending on the current work in progress of the REWIRE project, information can be added/edited/removed from this tool.





² <u>https://www.enisa.europa.eu/topics/education/ewigpeap-cybersecurity-skills-framework</u>

REWIRE – Cybersecurity Skills Alliance A New Vision for Europe

Home Job Ads Analyzer CyberSecurity Profiler Childen International Security Opencer (CIS)	12 EESE Roles	CYBER I EGAL POLICY & COMPLIANCE OFFICER	8
CYBER THEFAT INTELL INSENCE SECIAL IST			
Cybersecurity Architect			
Alternative Title(s) Summary Statement Mission Deliverables Main Task(s) Key Skill(s) -	Key Knowledge e-Competences	
Titles Cybersecurity Solutions Architect			
Cybersecurity Designer			
Data Security Architect			
	\$	4	
CYBERSECURITY EDUCATOR	CYBERSECURITY IMPLEMENTER	CYBERSECURITY RESEARCHER	
	Figure 9 - ECSF Explore	er	

1.2.4. Career Path / Development

The Career Path/Development tool is designed to help users self-manage their career path and development, simply by targeting a Cybersecurity Role profile. This tool is very easy to use as it consists of 4 simple steps, which are illustrated in figures 10, 11, 12 and 13, respectively, where users can navigate by selecting boxes and clicking the "Next" button. At each step they are allowed to go back to the previous one by clicking the "Back" button.

- 1. **Role Selection:** users can choose one of the 12 ECSF roles explored in the ECSF Explorer tool, namely:
 - Chief Information Security Officer (CISO)
 - Cyber Incident Responder
 - Cyber Legal, Policy & Compliance Officer
 - Cyber Threat Intelligence Specialist
 - Cybersecurity Architect
 - Cybersecurity Auditor
 - Cybersecurity Educator
 - Cybersecurity Implementer
 - Cybersecurity Researcher
 - Cybersecurity Risk Manager
 - Digital Forensics Investigator
 - Penetration Tester

PUBLIC

- 2. **Skills Selection:** depending on the role selected in the first step, a different list of skills appears, from which users can select those they already own.
- 3. **Knowledge Selection:** similarly, users can select the knowledge they already possess from the list displayed in this step.
- 4. Cybersecurity Career Pathway: a list of skills and knowledge that remain to be acquired so that users can reach their desired role they selected in step one. For further assistance, the tool invites users to navigate the official REWIRE project platforms of Cyber Range³, Online Courses⁴ and Certification⁵ to continue their upskilling/reskilling journey. Finally, as shown in figure 14, in this last step users have the option to export the results to a pdf file, which is illustrated in figure 15, by clicking on the "Export" button.

😁 REWIRE 🏠 Home Job Ads Analyzer CyberSecurity Profiler	12 ECSF Roles Career Path/Development		🕗 🛛 Log in
Desired Role	Acquired Skills	Acquired Knowledge	Missing Requirements
	Role Select	tion	
	Select the cybersecurity-related role you	are aiming to achieve.	
	E Chief Information Security	Officer (Ciso)	
	🛛 💋 Cyber Incident Responder		
	□ 🖉 Cyber Legal, Policy & Com	pliance Officer	
	Cyber Threat Intelligence Spectrum	pecialist	
	Cybersecurity Architect		
	Cybersecurity Auditor		
	Cybersecurity Educator		

Figure 10 - Career Path/Development, Step 1 – Role Selection, example of Cyber Incident Responder role



PUBLIC



³ <u>https://rewireproject.eu/cyber-range/</u>

⁴ <u>https://vle.rewireproject.eu/</u>

⁵ <u>https://rewireproject.eu/certification/</u>

REWIRE & Home Job Ads	Analyzer CyberSecurity Profiler 12 ECSF Roles Career Path/Develop	ment	Log in			
Desired Role	Acquired Skills	Acquired Knowledge	Missing Regulrements			
	Cyber Incid	ent Responder				
	Skills Selection					
	Choose the skills you already own.					
	Collaborate with other team members and colleagues					
	Communicate; present and report to relevant stakeholders					
Develop and communicate, detailed and reasoned investigation reports						
	Practice all technical, functional and operational aspects of cybersec	urity incident handling and response				
	Manage and analyse log files					

Figure 11 - Career Path/Development, Step 2 – Skills Selection, example of Cyber Incident Responder role

REWIRE	urity Profiler 12 ECSF Roles Career Path/Development		💿 🛛 Log in			
Desired Role	Acquired Skills	Acquired Knowledge	Missing Requirements			
	Cyber Inciden	t Responder				
	Knowledge Selection					
	Choose the knowledge subje	cts you already possess.				
	Secure Operation Centres (SOCs) operation					
	Computer Security Incident Response Teams (CSIRT	s) operation				
□ Incident handling standards, methodologies and frameworks						
	Incident handling recommendations and best practice	es				
	Incident handling tools					

Figure 12 - Career Path/Development, Step 3 – Knowledge Selection, example of Cyber Incident Responder role

REWIRE 🛆 Home Job Ads Analyzer	CyberSecurity Profiler 12 ECSF Roles Career Path/Developmen		E Login				
Desired Role	Acquired Skills	Acquired Knowledge	Missing Requirements				
Cyber Incident Responder							
Cybersecurity Career Pathway							
Good job so far! This is what rem	ains to be acquired to reach your desired role. Check out	the REWIRE Cyber Range, Online Courses, and Certific	cation to help you achieve your goal.				
Missing Skills							
Practice all technical, functional and operational as	pects of cybersecurity incident handling and response						
Manage and analyse log files							
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements							
Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks							
Analyse and comply with cybersecurity-related laws, regulations and legislations							
Understand, practice and adhere to ethical requirements and standards							
Inderstand leval framework modifications implications to the organisation's cybersecurity and data protection strategy and policies							

Figure 13 - Career Path/Development, Step 4 – Cybersecurity Career Pathway output, example of Cyber Incident Responder role

🤤 🔛	EWIRE	습 Home	Job Ads Analyzer	CyberSecurity Profiler	12 ECSF Roles	Career Path/Development		Log in	
	Responsible information disclosure procedures								
	Offensive and c	lefensive secur	ity practices						
	Offensive and defensive security procedures								
	Computer networks security								
	Cybersecurity p	olicies							
	Cybersecurity s	tandards, meth	nodologies and frame	works					
	Cybersecurity r	elated laws, reç	gulations and legislati	ions					
	Cybersecurity-r	elated certifica	tions						
	Legal, regulator	y and legislativ	ve compliance require	ments, recommendation	is and best practic	es			
	Legal, regulator	y and legislativ	ve requirements on re	leasing or using cyberse	curity related tech	nologies			
	Ethical cybersecurity organisation requirements								
	Operating syste	ms security							
	Advanced and	persistent cybe	r threats (APT)						
	Cyber threats								
	Cybersecurity a	ttack procedur	es						
	Threat actors T	actics, Techniq	ues and Procedures ((TTPs)					
	Cyber threat ac	tors							
Back								Export	

Figure 14 - Career Path/Development, Step 4 – Cybersecurity Career Pathway, export to pdf option



Cyber Incident Responder

Cybersecurity Career Pathway

Good job so far! This is what remains to be acquired to reach your desired role. Check out the REWIRE Cyber Range, Online Courses, and Certification to help you achieve your goal.

Missing Skills				
- Manage and analyse log files				
omprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements				
Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks				
Analyse and comply with cybersecurity-related laws, regulations and legislations				
Work ethically and independently; not influenced and biased by internal or external actors				
Work on operating systems, servers, clouds and relevant infrastructures				
Missing Knowledge				
Incident handling communication procedures				
Offensive and defensive security practices				
Cybersecurity policies				
Cybersecurity-related certifications				
Legal, regulatory and legislative compliance requirements, recommendations and best practices				
Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies				
Advanced and persistent cyber threats (APT)				

Figure 15 - Career Path/Development, Step 4 – Cybersecurity Career Pathway, pdf document example of Cyber Incident Responder role

1.3. Access and documentation

The CyberABILITY platform is available in the main menu of the official REWIRE project website⁶ or directly here⁷.

Finally, the demonstration of the use of tools is available on the REWIRE project YouTube channel⁸.





⁶ https://rewireproject.eu

⁷ https://rewireproject.eu/cyberability/

^{* &}lt;u>https://rewireproject.eu/cyberability/</u> PUBLIC * <u>https://www.youtube.com/channel/UC2-zInGvTsUOB5F5dM2IHtw</u>