



Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions

Security-by-design for end-to-end security

H2020-SU-ICT-03-2018



Cyber security cOmpeteNCe fOr Research andD InnovAtion[†]

CONCORDIA Course “Becoming a Cybersecurity Consultant”

The Pilot – structure and deployment

Abstract: This document describes the pilot course “Becoming a Cybersecurity Consultant” in terms of structure and its deployment. It also contains details on the feedback received from the participants to the pilot, and the next steps envisioned to be taken in year 2021.

Editor	<i>Felicia Cutas</i>
Contributors	<i>EIT Digital – Felicia Cutas TUVA - Argyro Chatzopoulou UL – Lama Sleem</i>

[†] This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

Table of Contents

1	INTRODUCTION.....	3
1.1	FROM A ROLE PROFILE TO A COURSE CURRICULUM	3
1.2	STRUCTURE OF THE COURSE AND CONTRIBUTION.....	4
2	THE PARTICIPANTS FUNNEL	5
3	THE ONLINE MODULE	6
3.1	STRUCTURE.....	6
3.2	DEPLOYMENT	7
3.3	FEEDBACK RECEIVED	7
4	THE LIVE WEBINAR	10
4.1	STRUCTURE.....	10
4.2	DEPLOYMENT	10
4.3	FEEDBACK RECEIVED	11
5	NEXT STEPS.....	13

1 Introduction

The course “Becoming a Cybersecurity Consultant” was developed and deployed by applying elements of the CONCORDIA Methodology for creating courses for cybersecurity professionals [\[Link\]](#) applied to the Cybersecurity Consultant role profile, and its pilot was deployed in the period January 21st – May 13th, 2021.

Since the role of the Cybersecurity Consultant has been identified as intermediate in level, the course also was directed to professionals already active in the cybersecurity or individuals having already some basic knowledge in cybersecurity.

1.1 From a Role Profile to a course Curriculum

This course travelled in unmapped territory, since no profile for the Cybersecurity Consultant existed prior to this effort in Europe. The document CONCORDIA Workshop on Education for cybersecurity professionals - post workshop report – [\[Link\]](#) depicts the process followed by the CONCORDIA project to construct and validate the Cybersecurity Consultant Role Profile.

The implemented profile was expressed in a manner compatible to both the NICE Cybersecurity Workforce Framework taxonomy [\[Link\]](#) and the European e-Competency framework [\[Link\]](#). Due to the maturity of the NICE Cybersecurity Workforce framework, the project team selected to construct the curriculum based it and identified 73 Knowledge and 38 Skills requirements.

Since the course was proposed for professionals at a medium level, considering the limited time a professional could allocate for upskilling thus the need to get focused and the most in demand information, the knowledge and skills requirements were prioritized based on their importance during the relevant workshop [\[Link\]](#). The selected, most important, knowledge and skills were aggregated and grouped under three main learning objectives:

1. Threats – Get updated on the existing and emerging cybersecurity threats, the assets possible to be impacted, and the latest models of attacks.
2. Technology – Become knowledgeable about specific technological threats, learn how to anticipate and prevent them, while developing proactive management skills.
3. Economics – Get an understanding of the economics behind cybersecurity activities within your organization. Learn about risk management and information security to protect the corporate reputation and preserve customer loyalty.

The following figure depicts the knowledge and skills covered by the Cybersecurity Consultant course curriculum per learning objective (as stated above).



List of Knowledge and Skills addressed under the 3 main learning Objectives

Opportunity for Improvement: A role profile (especially one following the NICE framework) usually contains an increased number of identified as required Knowledge, Skills and Abilities. In a professional course that should be completed within a definite and short period of time, a selection process has to be implemented, to define the learning objectives and filter down the knowledge, skills and abilities the course will bestow on the participants. In this case, the selection process contained one criterion – importance of the Knowledge, Skill and Ability.

Based on the performance of the pilot course, it was derived that the Knowledge, Skill and Ability should also be filtered using the following criteria:

- Pre-requisite (Knowledge, Skill or Ability) (based on the level of the role)
- Alternative methods to acquire the relevant requirement (outside the course) and
- Suitability for the specific type of course (e.g., theoretical classroom based, practical, on the job etc.)

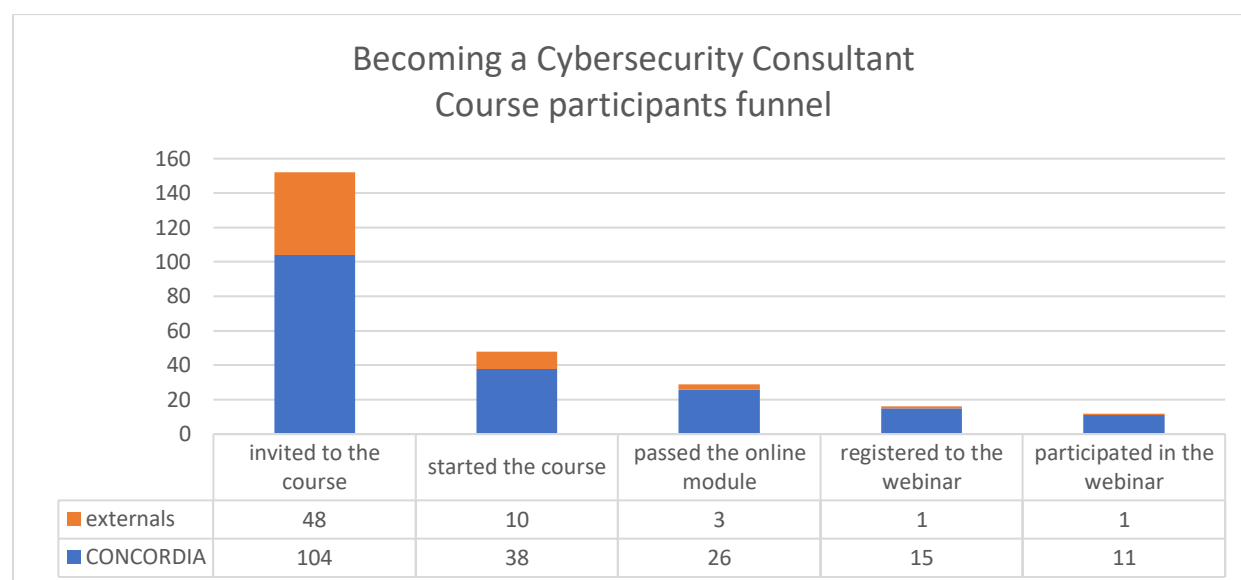
The course is structured in two parts: online and face-to-face. Due to the COVID-19 restrictions, the face-to-face module of the pilot course was organized as a live webinar.



The activity was coordinated by EIT Digital and received substantial support in all its phases, from design to implementation, from CONCORDIA academic and industry partners: University of Milan, Italy; University of Lorraine, France; University of Zurich, Switzerland; The Industrial System Institute, Greece, University of Insubria, Italy; BITDEFENDER, Romania; Arthur's Legal, The Netherlands. Since the pilot course was developed and deployed in conjunction to the pilot Cybersecurity Skills Certification scheme, the process required a close collaboration with TÜV Trust IT GmbH, member of the TÜV Austria Group.

2 The participants funnel

To run the pilot, we invited all the CONCORDIA partners to attend it and provide feedback (we limited the participation to 2 people per partner for convenience). As a courtesy, we also extended the invitation to the external participants who attended the webinar in June 2020 [\[Link\]](#) and contributed to the definition of the Cybersecurity Consultant role profile.



From the 150 people invited, 48 of them decided to enroll in the online part of the course and 29 participants managed finish the module (score 80% or higher to the quizzes part of the online module). We then proceeded to invite all the 29 successful learners to register for the second part of the course but only 12 of them finally managed to accommodate their agenda to the live event. The participants funnel is depicted in the image on the left.

Out of the 12 participants to the webinar, 4 were coming from the industry, 5 represented universities or research organizations and 3 were coming from other type of professional cyber-related entities.

3 The online module

3.1 Structure

The online part of the course was designed to cover theoretical concepts a Cybersecurity Consultant (medium level) should know. Since the different Knowledge and Skills targeted by the course were aimed at being covered through different angles, we decided to structure the online module around 4 big themes: Cybersecurity Principles; Offensive Methods; Defensive Methods; Risk Management. Each of the lessons part of a module is covering a set of knowledge and skills part of one, two or even all three learning objectives as mentioned in the table below.

Module	Lesson code	Lesson title	Learning Objective
A - CYBERSECURITY PRINCIPLES	A1	CIA Triad and Security Principles	LO1, LO2
	A2	Software Vulnerabilities: CVE, CVSS, and beyond	LO1
	A3	Privacy Principles to Manage Risks Related to Data	LO1
	A4	Accountability as success factor in this Digital Age	LO1, LO2, LO3
B -OFFENSIVE METHODS	B1	Attacks Capabilities and Attacks Stages	LO1
	B2	Emerging Security Issues and Evolving Attacks	LO1
	B3	Network Attacks	LO2
	B4	Internet Technologies: Definition, Principles and Top Threats	LO2, LO3
C - DEFENSIVE METHODS	C1	The Security by design Principle Approaches and Paradigms	LO1
	C2	Vulnerability Management Methods	LO2, LO3
	C3	Network Protections Methods	LO2, LO3
	C4	OS/Application Protections Methods	LO2, LO3
	C5	Data Protection and Security	LO3
	C6	The SIM Approach	LO2, LO3
D - RISK MANAGEMENT	D1	Overview on Risk Assessment Framework	LO1, LO3
	D2	Risk Management with an Economic Bias	LO3
	D3	Non-conformity/non compliance perspectives	LO3
	D4	Digital Sovereignty	LO1, LO2, LO3

List of the lessons part of the pilot course – online module

The content is proposed to be completed in about 3-4 weeks-time while allocating about 2-3 hours a week.

B1 - Attacks Capabilities and Attacks Stages

Video: Introduction

Published

7m 1 Objective

Video: Cyberattack lifecycle: Before the Attack

Published

11m 1 Objective

Quiz: Cybersecurity lifecycle: Before the attack

Published

4m

Video: Cyberattack lifecycle: During the Attack

Published

15m 1 Objective

Video: Cyberattack lifecycle: After the Attack

Published

6m 1 Objective

Quiz: Cyberattack lifecycle: During and After the Attack

Published

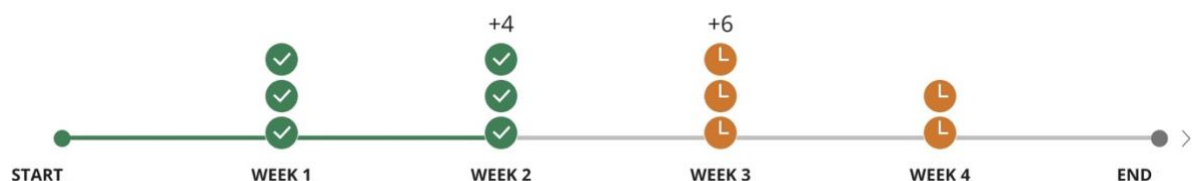
3m

Each individual lesson was covered over 2-5 short videos of about 5-15' length. As a general rule, we have inserted quizzes to help revise some of the important concepts after video slots of approx. 15' length. An example of the structure is depicted in the image on the left.

The online module of the pilot course contained a total of 18 lessons deployed over 57 videos and 21 quizzes, covering about 9 hours of content.

3.2 Deployment

The online module was hosted under the COURSERA platform and was open in private mode between January 21 – March 8. The content (lessons and quizzes) was structured and automatically proposed to be taken over a period of 4 weeks with reminders set accordingly and sent automatically to the participants by the platform. Yet, the learners were able to follow the lessons and take the quizzes at their own pace since all the content was fully accessible from the beginning of the period until the very last day. The figure right below displays a view from the Coursera platform where the learners could monitor by themselves their progress with respect to the quizzes taken or still to be taken.



Learner view on the structure of the quizzes over 4 weeks interval

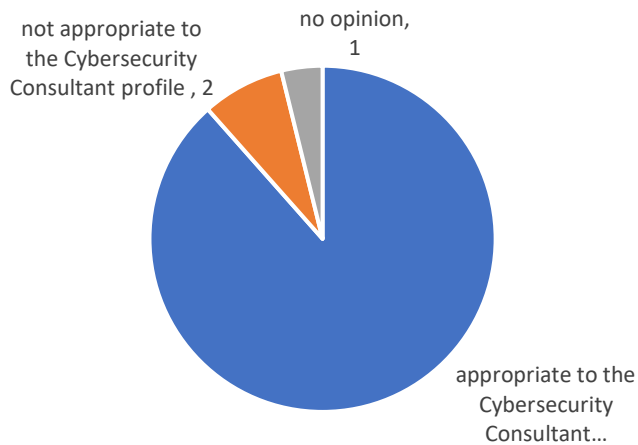
Considering the level of the profile addressed, we decided to set the pass mark for the quizzes at 80%.

3.3 Feedback received

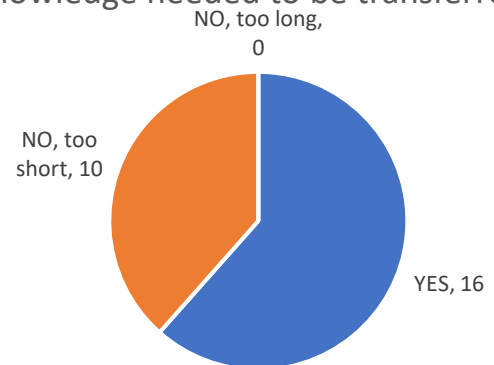
The participants to the online module of the course were invited to provide their feedback as part of the continual improvement process of the course. Out of the 48 participants, 26 filled in the feedback form.

The participants answered both multiple choice questions and open questions regarding the structure and the content covered by the lessons, through the perspective of the role profile: Cybersecurity Consultant medium level.

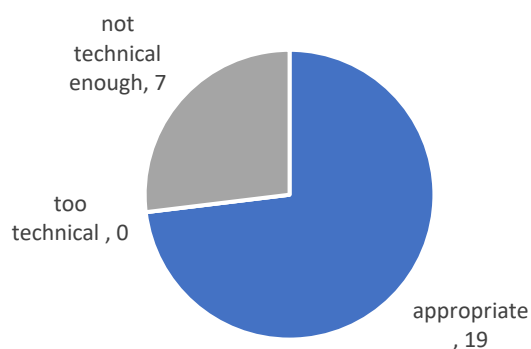
Q1: How did you find the **overall structure** of the course?



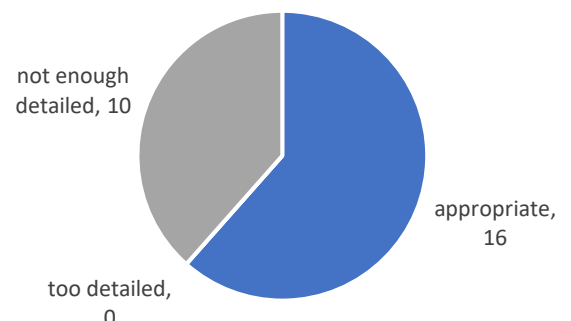
Q2: Is the **total length** of the course appropriate to the volume of knowledge needed to be transferred?



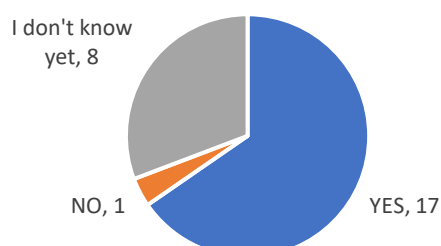
Q3: How did you find the **type of knowledge** presented in the course for Cybersecurity Consultant profile - medium level?



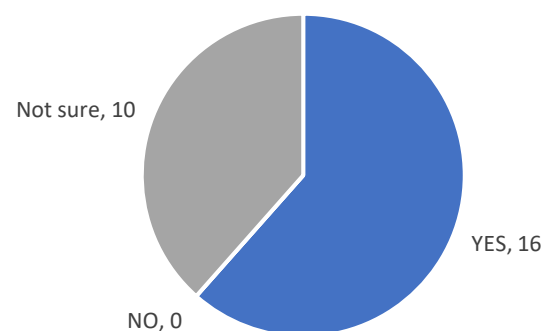
Q4: How did you find the **depth of knowledge** presented in the course for Cybersecurity Consultant profile - medium level?



Q5: Would you be interested to attend the live **webinar** providing more in-depth knowledge on the topics, presenting case studies and running hands-on exercises?



Q6: Would you be interested to apply for a Cybersecurity Consultant skills **Certification** Scheme?



Overall, the respondents confirmed that the structure of the lessons, and the total length of the online module are appropriate. With respect to the type and depth of knowledge covered they are confirmed that they were fitting the targeted profile.

The general comments were overall positive and very positive and included some useful suggestions. E.g.:

- *In general the course seems to cover fundamentals and some advanced cyber security aspects. Pretty good course design in this regard.*
- *This course is very well setup and the explanations are very clear. I like that we can see all the speakers through video, this is really great, and the user experience is a lot better like this!*
- *It is really a great advantage to listen to all the cybersecurity experts on one place, the topics are perfect and very well described.*
- *I would propose to start with an introduction focused on the "consultant role"... Yes, of course, cybersecurity consultant needs to know the basic terminology and principles, but we should give the learners the overreaching mental model about the role of cybersecurity consultant which will help them to connect the information in the course.*

We also requested the participants to suggest topics they consider relevant to be covered for the Cybersecurity role profile medium level and which currently are missing from the course. Between the proposals coming from participants, we find risk management, impact assessment, threat intelligence, legal landscape, ethics and third-party management.

Apart from the general observations we have also received very specific comments on individual lessons and quizzes. These comments will be considered for improving the course prior to its opening to the European market.

4 The live webinar

4.1 Structure

The Face-to-Face/webinar part of the course is designed to build on the theoretical concepts covered in the online part by bringing into the discussion of the group different case studies while also involving the participants in hands-on exercises.

Due to the restrictions imposed by the COVID-19 crisis, the face-to-face module was replaced with a live webinar.

The agenda of the 3 days pilot webinar module was structured as follows:

Day 1	Day 2	Day 3
<ul style="list-style-type: none">• Welcome• The Cybersecurity Consultant role profile• Risk assessment• Threats identification• Vulnerability analysis	<ul style="list-style-type: none">• Source code analysis• Penetration testing• Legal aspects	<ul style="list-style-type: none">• The Cybersecurity Economics• Risk Analysis with an Economic Bias• The Certification process• ISOGRAD and KYPO platforms• Closing

Two of the presentations part of Day 1 of the webinar, namely The Cybersecurity Consultant role profile and the Risk Assessment, were included as a response to the feedback we received from the online module.

The last presentations part of Day 3 of the webinar were dedicated to introducing the C³ by CONCORDIA Certification scheme attached to this course, and the platforms under which the theoretical and practical exams will run.

4.2 Deployment

The pilot live webinar ran between May 11th – May 13th and it covered 3 hours per day, from 16:00 till 19:00 CET. Because of the fix schedule, only 12 out of 29 people (having successfully finished the online module) were able to attend the webinar.

Most of the webinar sessions were hands-on and required an active participation of the learners. The exercises varied in style, from paper based to simulations on specialized platforms such as Moon Cloud and Kypo CRP and were time bound. In order to keep the participants fully engaged and motivated, we invited them to share their individual results via private channels (Slack) with the lecturer. The solutions were afterwards discussed with the whole group.

Since the platforms used during the webinar required individual authentication, we deployed a preparatory step prior to the webinar in order not to lose time during the lessons with the technical settings. Specifically, the participants received in advance of the event the necessary




credentials and clear instructions on how to setup their accounts and access the platforms, and they were asked to log-in in order to test their access.

4.3 Feedback received

We asked the participants to provide their feedback both on general aspects of the webinar as well as on each session.



Overall agenda

How would you rate the overall agenda of the webinar for Cybersecurity Consultant profile, medium level?

		Answers	Ratio
Very relevant		6	60%
Relevant		3	30%
Not relevant enough		1	10%
No Answer		0	0%



The length of the webinar

How would you rate the length of the webinar (3 half days, 3 hours each)

		Answers	Ratio
Long enough		5	50%
Too short		5	50%
Too long		0	0%
No Answer		0	0%

The depth of the content

How would you rate the depth of the content presented during the webinar for the targeted profile?

		Answers	Ratio
Appropriate		8	80%
Too technical		0	0%
Not technical enough		2	20%
No Answer		0	0%

When it comes to the assessment of the individual sessions, the participants' answers to the question "How would you rate the exercises ran / examples offered during the webinar" converged towards:

- Relevant to Very relevant - in terms of Relevance for the targeted profile
- Appropriate – in terms of Difficulty for the targeted profile
- Very clear to Clear – in terms of Explanations offered by the lecturers.

Apart from these structured answers we have also collected qualitative input via open questions. Specifically, we invited the participants to share 3 things that they liked in this webinar and 3 things that they didn't really like in this webinar.

Between the elements they liked to the webinar are: the practical approach, the Economics topics and the platforms used (KYPO and Slack). With respect to the elements they didn't really like and suggested to change and /or improve where: the length the webinar which was considered too condensed and the speed view by some of the instructors, the need for more

exercises and more clear instructions on how to use the platforms to be sent out prior to the event.

We also encouraged the participants to leave some testimonials for the future potential participants to the course:

"Gain hands-on experience on evaluating and dealing with protection of assets and get a chance to discuss with other experts on the field of cybersecurity."

"The course is well laid out and organized into different modules, with a lot of interesting details in each module included, and quizzes to keep you engaged with the content. Also, the exercises in the hands-on sessions are cool and can entice your interest to look into these tools further, beyond the duration of the course."

"A great overview with practical examples of how to tackle security in cyberspace."

"This was exactly what I needed to improve my knowledge in cybersecurity"

"One of a kind! State of the art tools and technologies presented in a comprehensive manner! A must have for any cybersecurity professional!"

"Even some of the topics may look easy or too common, it is very important to have such a course that puts all these things together."

"Great seminar to start your cybersecurity consultant career in which you will learn from a variety of topics covering a wide aspect of security from technical to financial."

"Very well-structured course, offers a complete overview of the several cybersecurity aspects. Perfect for beginners."

5 Next steps

Following the feedback received from the participants we will look into improving the content of the course by, for instance, adding new lessons and offering more space for hands on exercises.

In support to a better communication of the content and deployment of the course we have created a specific webpage introducing all the different aspects associated to the targeted role profile, the course itself, and the associated Certification scheme C³ by CONCORDIA.



Print-screen of the web-page <https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/>

Between June 1st - July 14th we ran the pilot Certification Scheme via a proctored theoretical exam and a practical exam. The results of this pilot will be the subject of a separate report.

The first open session of the course is schedule to start in October 2021. In view of reaching out to as many potential participants as possible, we have opened a pre-registration form already in mid-June. The pre-registration was/is promoted it via the CONCORDIA newsletter and European Commission specific Cybersecurity newsletter, and on social media. By end of July we have already received pre-registrations from 35+ individuals from 14 European countries, more than half of them representing Corporates, SME/startups and freelancers.