CYBERWISER.eu, www.cyberwiser.eu | @cyberwiser

CYBERWISER.eu INTERMEDIATE:
A new personalised cyber-risk training course with cyber range scenarios

The CYBERWISER.eu INTERMEDIATE offering level is now available, designed to help organisations combat cyber-threats in today's evolving landscape with the increasing use of digital and virtual applications. This offering level takes employees up a gear with detailed and specific training, just right in the new normal of remote working and growing use of personal devices and networks. CYBERWISER.eu INTERMEDIATE is for IT-reliant organisations that need the right skills to protect their data and assets, as well as faster response times to new vulnerabilities, which malicious hackers and cybercriminals are all too keen to exploit.
According to the IBM Data Breach Report, the average cost of a data breach in 2020 was $3.86M. The average time to identify and contain it was 280 days. A staggering 76% of organisations facing a cyber-attack had shifted to remote work.
Even once the Pandemic is over, many employees are likely to continue working from home, with possible increases in the costs of a data breach.
Organisations, small and large, need to move highly effective cybersecurity training up their priority list so their data and IT assets are kept safe from harm.

CYBERWISER INTERMEDIATE - target groups

CYBWERWISER.eu intermediate is designed for more experienced and expert users coming from SMEs, large companies, and public sector organisations.
The intermediate level meets the following needs:

- **SMEs:** Professionals that already have an understanding of the basic concepts and good practices (e.g., what to avoid/look out for in everyday tasks such as fraudulent emails etc.). Especially IT, network, and cyber specialists who need to improve in threat and vulnerability analysis as well as respond to cyber-attacks and incidents.
- **Large companies:** Professionals that have more complex cybersecurity needs, such as guaranteeing efficiency, business continuity, and intellectual property, among other assets. CYBERWISER.eu Intermediate can provide a secure environment to simulate attacks and enable trainees a good grounding in incident response and testing, including profiles like security operations centre (SOC) analysts.
- **Public sector organisations:** From administrations and healthcare IT to public safety, CYBERWISER.eu Intermediate, helps public-sector professionals hone the skills they need to protect their IT assets through both awareness campaigns and customisable training solutions. Organisations can also train an in-house team of cybersecurity experts.

The courses within the Offering Level

The Intermediate offering level offers the user a much more personalised experience thanks to cyber range training scenarios, a suite of automated cyber-attacks and the vulnerability assessment tools. Additionally, in these offering level the user can exploit parameter-based **real-time evaluation of trainee performance** supported by models and algorithms for **economic risk evaluation**.
Other aspects of context establishment, cyber-risk assessment, cyber-risk treatment, and cost/benefit analysis will be covered.

In particular the the user of this offering level will go through the following topics:

- **Describe target of analysis, level 2**
    - Understand how to use UML class diagrams
    - Apply the relevant assets on the CYBERWISER.eu cyber range to create simulated infrastructure
- **Identify risk criteria**
    - Define likelihood scales.
    - Define consequence scales for each information security asset.
    - Define risk evaluation criteria and corresponding risk evaluation matrix.
    - Cyber-risk reports on CYBERWISER.eu
- **Identify risks, level 2**
    - Identify risk indicators.
    - Obtaining indicator values in CYBERWISER.eu
    - Cyber-risk models in support of cybersecurity training and evaluation.
- **Estimate risks**
    - Likelihood and consequence estimation.
    - How to update risk assessment algorithms?
- **Treat risks, level 1**
    - Identification risk through CORAS model.
    - Associate risk treatments on vulnerabilities
    - Analyse a risk model and create appropriate risk treatments

About CYBERWISER.eu

CYBERWISER.eu, www.cyberwiser.eu/, is an Innovation Action co-funded by the European Commission, H2020 Programme, under Grant Agreement 786668.

The Consortium is composed by 9 domain-skilled partners from 7 European Countries: Spain: (ATOS), United Kingdom (Trust-IT Services), Norway (SINTEF), Slovenia (XLAB), Italy (Ferrovie dello Stato Italiane, Università di Pisa, AON), Portugal (EDP) and Belgium (RHEA Group), bringing together a nice mix of large companies, SMEs, research and educational institutions.

CYBERWISER.eu expands and builds on the success and strong user community of the H2020 Innovation Action WISER (2015-2017), helping to accelerate awareness-raising and jump-start earlier investments.