COMPACT

CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

Grant Agreement: No 740712
Project Acronym: COMPACT
Project Title: COmpetitive Methods to protect local Public Administration from Cyber security Threats
Thematic Priority: Secure societies – Protecting freedom and security of Europe and its citizens
Start Date: May 1st, 2017
Duration: 30 months
Total cost: EUR 4 283 480
EU contribution: EUR 3 648 792,50

www.compact-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740712

Cybersecurity Awareness Training. A Gamified Approach.

Cybersecurity Awareness Training Tools

- John Dewey’s “Learning by doing" approach:
  - To improve the student's motivation and lead to deeper understanding and learning.
- The strengthening of the weakest link in the security chain elevates the cyber-security level of the LPA:
  - COMPACT aims to increase the cybersecurity awareness of LPA employees, by educating them about the cyber-risks they are most exposed to and by empowering them to decide which approaches to adopt.
- The COMPACT modules on Security Awareness Training embrace the gamification approach
  - To be more attractive to employees;
  - Customized for specific categories of LPA employees:
    - Gender issues, personality traits and more.

- **OPENNESS.EDU**
- **SOLE**
- **CYBERRANGE**
- **SECTOPIA**
- **INVESTIGATION DIARY**
- **KIPS**
- **CSMG**

OPENNESS.edu

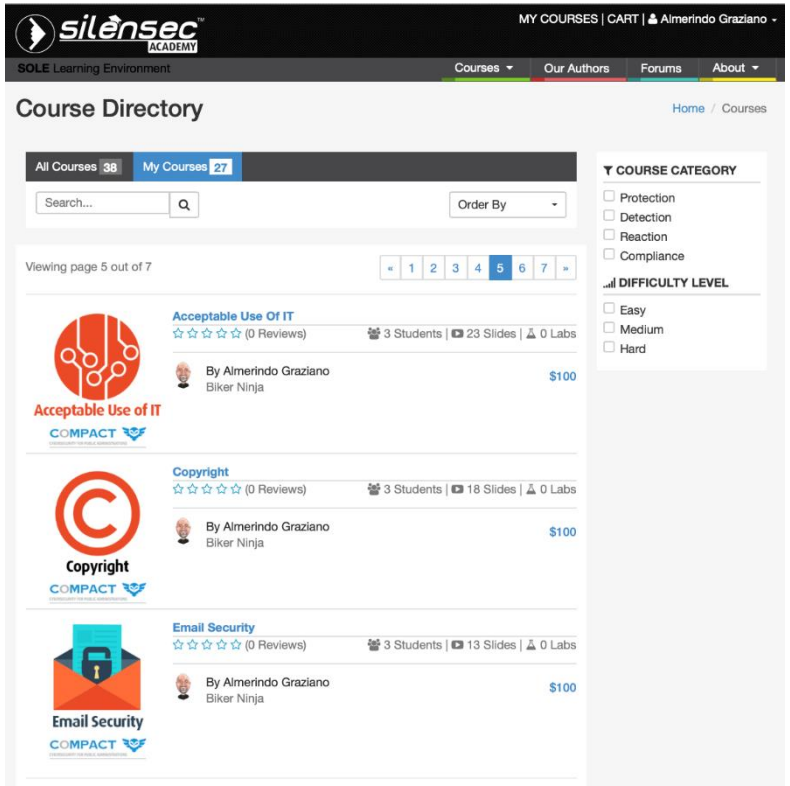
- Catalogue of trainings and educational services
- Career storage
- Targets: all the employees of an organization

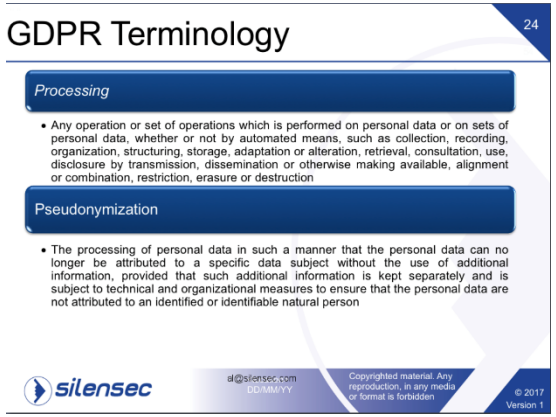
- SaaS
- Collects external providers' scores and grades (SOLE, CSMG, KIPS…)

SOLE - Silensec Online Learning Environment

- Cloud-based E-learning platform
- Hands-on labs
- Security awareness assessment
- SaaS Model

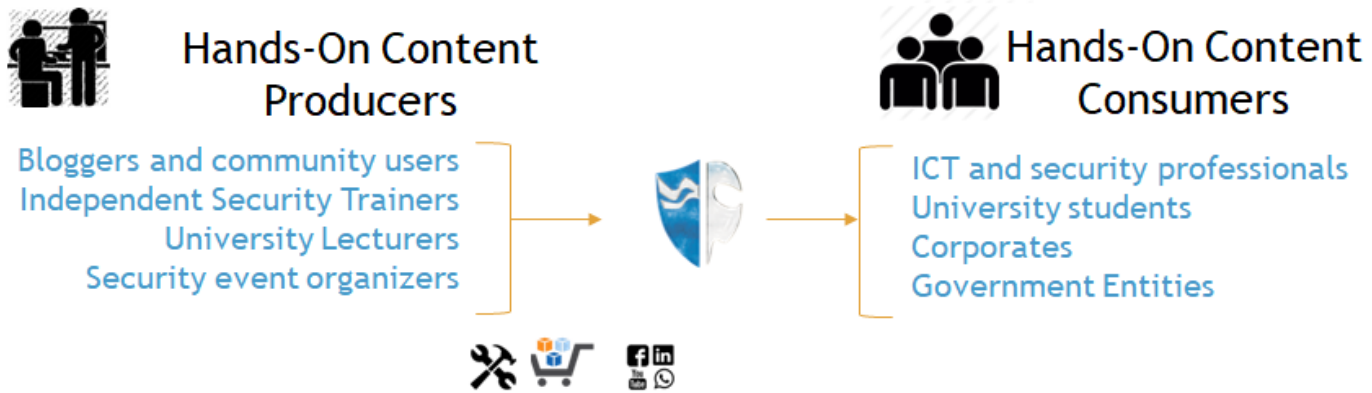
- New Courses for COMPACT end users:
  - GDPR Compliance
  - MISP for COMPACT
  - Using OpenIntel





Silensec CyberRange

- Cyber Range is a marketplace for hands-on content delivered on top of a proprietary cloud-based cyber range platform.
- Silensec Cyber Exercises design: each scenario is uniquely designed to meet specific objectives and tailored for a specific target audience.
  - Identification of the skills and competences to asses;
  - Design and development of realistic environments and scenarios and the associated set of challenges and tasks to be carried out.
- Cyber Range is used within the COMPACT Project to deliver scenarios to test the level of security awareness of LPAs.



- **What is a Cyber Range?**

  A cyber range is a virtual environment simulating organization's networks, systems and applications, and providing a safe environment for cybersecurity training and product testing.

- **Why are Cyber Ranges Important?**

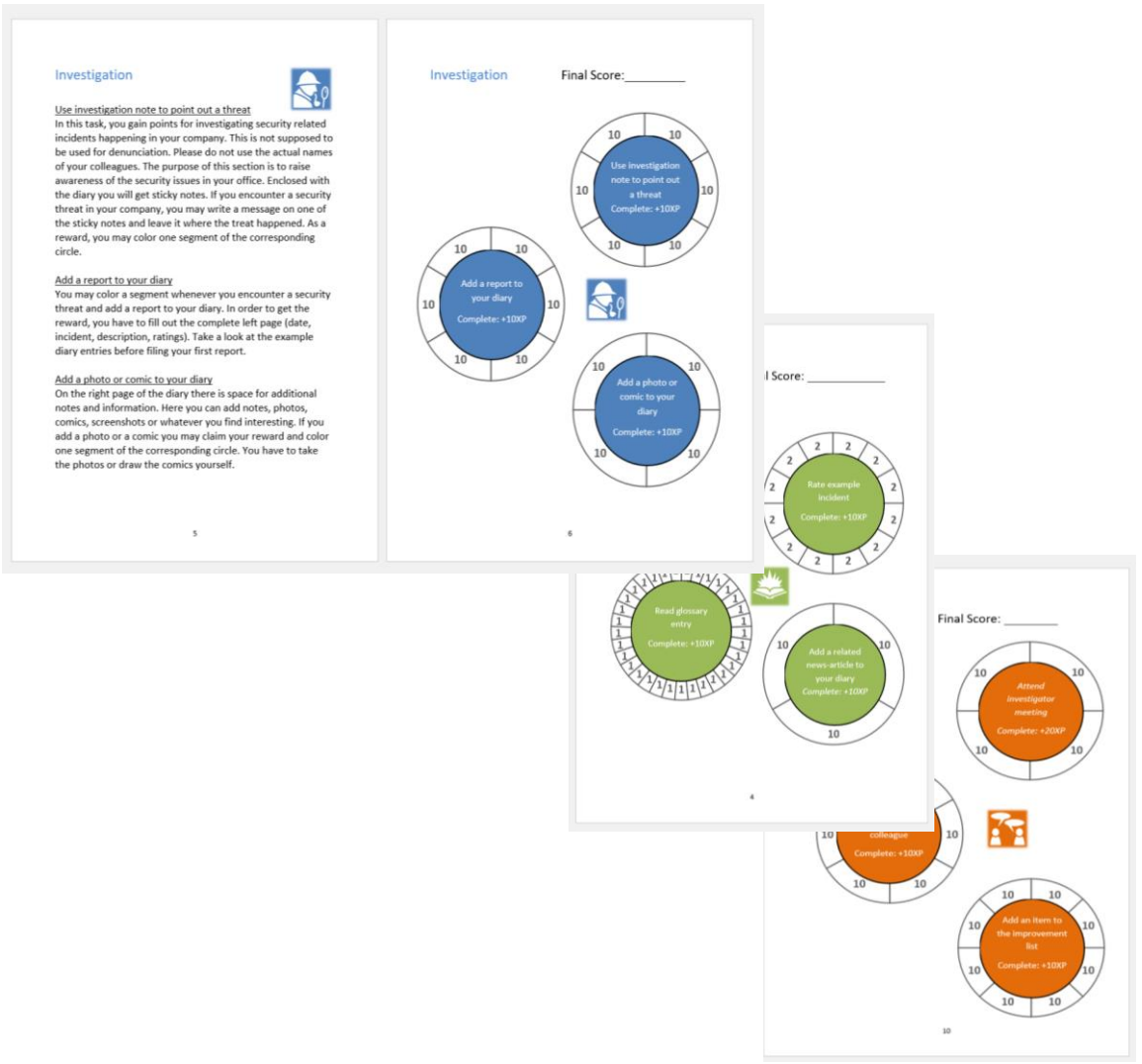
  Gartner: by 2022, 15% of large enterprises will be using cyber ranges to develop the skills of their security teams.

SECTOPIA

- **Sectopia** is a web-based serious single-player game that provides knowledge of social engineering threats and raises awareness of cybersecurity.
- The player take on a middle management position, having to decide whether certain actions of other employees are allowed according to security guidelines.

INVESTIGATOR'S DIARY

- **The Investigator's Diary** is a gamified awareness tool.
- Teams of about 5 people have to look for security risks in their organisation, learn security guidelines, interact with their colleagues, and solve tasks related to cybersecurity.
- They get points for knowledge acqusition, investigation, social interaction



Kaspersky Interactive Platform Simulation: KIPS

- **Gamified Training Target**: to preserve the LPA's reputation by maintaining cybersecurity.
  - Business Decision Makers act like a new Cybersecurity Team of the LPA scenario.
- **Idea**: build a cyber-defence strategy:
  - Dealing with threats;
  - Choosing from pro-active and re-active actions;
  - Complying with operational constraints - time and costs.

- A trainer conduct the game, to raise players awareness of security issues, GDPR included.
- Players get used to security controls
  - Audit, SIEM, AntiVirus, etc.
- Fun, engaging and fast: 2 hours.
- Team-work builds cooperation.
- Competition fosters initiative & analysis skills
- Gameplay for understanding security measures.

- The game is integrated with the COMPACT **Openness.edu** platform.
  - Links to the Trainer's console
  - Links to the Player's console
  - Game scores

Kaspersky CyberSafety Management Games - CSMG

- **Gamified Training Target**: to promote cyber-secure decision making among LPA employees.
  - Competence, knowledge and attitudes to maintain a secure working environment.
  - It covers all major security domains and typical situations at workplaces.
- **Idea**: transforming misconceptions into the adequate perception:
  - It gives to players positive behavior patterns.

- A trainer conduct the game:
  - A typical LPA workplace with 12 marked Zones;
  - A Zone contains potential cyber-threats.
- Participants put “casino-style” bets on all the Zones
  - Their reputation is at stake.
- Gameplay for learning to judge everyday situations.
- It fosters collaboration and competition.

- The game is integrated with the COMPACT **Openness.edu** platform.
  - Links to the Trainer’s console
  - Links to the Player’s console
  - Game scores

COMPACT consortium partners 14 organisations from seven EU countries.

Austria | Belgium | Cyprus | Germany | Italy | Portugal | Spain

Project Coordination:

Paolo Roccetti

Engineering Ingegneria Informatica spa

Via Riccardo Morandi, 32 - 00148 Roma

E-mail: paolo.roccetti@eng.it

Technical Coordination

Luigi Romano

Consorzio Interuniversitario Nazionale per l'Informatica

Via Salaria, 113 - 00198 Roma

E-mail: luigi.romano@uniparthenope.it

Grant Agreement: No. 740712
Project Acronym: COMPACT
Project Title: COmpetitive Methods to protect local Public Administration from Cyber security threats
Thematic Priority: Secure societies – Protecting freedom and security of Europe and its citizens
Start Date: May 1st, 2017
Duration: 30 months
Total cost: EUR 4 283 480
EU contribution: EUR 3 648 772,50

www.compact-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740712