
SIMARGL

Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware

Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833042

The Project

The mission of the SIMARGL is to provide new innovative advanced solutions to effectively fight malware, stegomalware, ransomware, badware, mobile malware and other malicious activities in computer networks and applications. SIMARGL will offer the integrat ed and validated toolkit improving European cyber security.

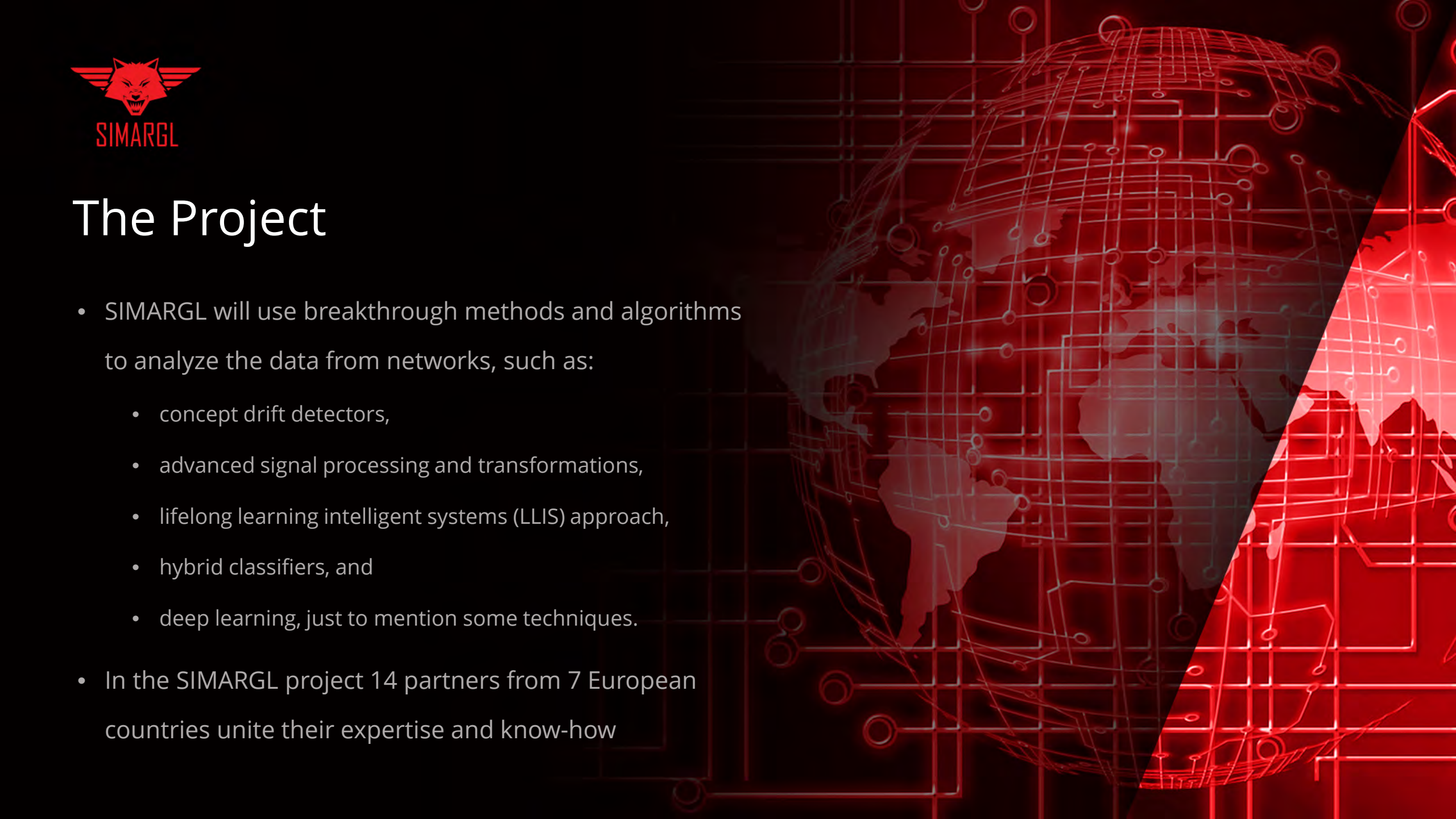
KEY FACTS:

- SIMARGL: Grant agreement ID: 833042
- Funded under: H2020-EU.2.1.1
- Duration: 1 May 2019 - 30 April 2022
- Overall budget: € 6 076 050, EU contribution € 4 984 260
- Coordinated by: FernUniversität in Hagen (Michał Choraś)

SIMARGL

The Project

- Co-funded by the European Commission under Horizon 2020 programme,
- The objective is to combat the pressing problem of malware.
- It aims to tackle the new challenges in the cybersecurity field, including information hiding methods, network anomalies, stegomalware, ransomware and mobile malware.



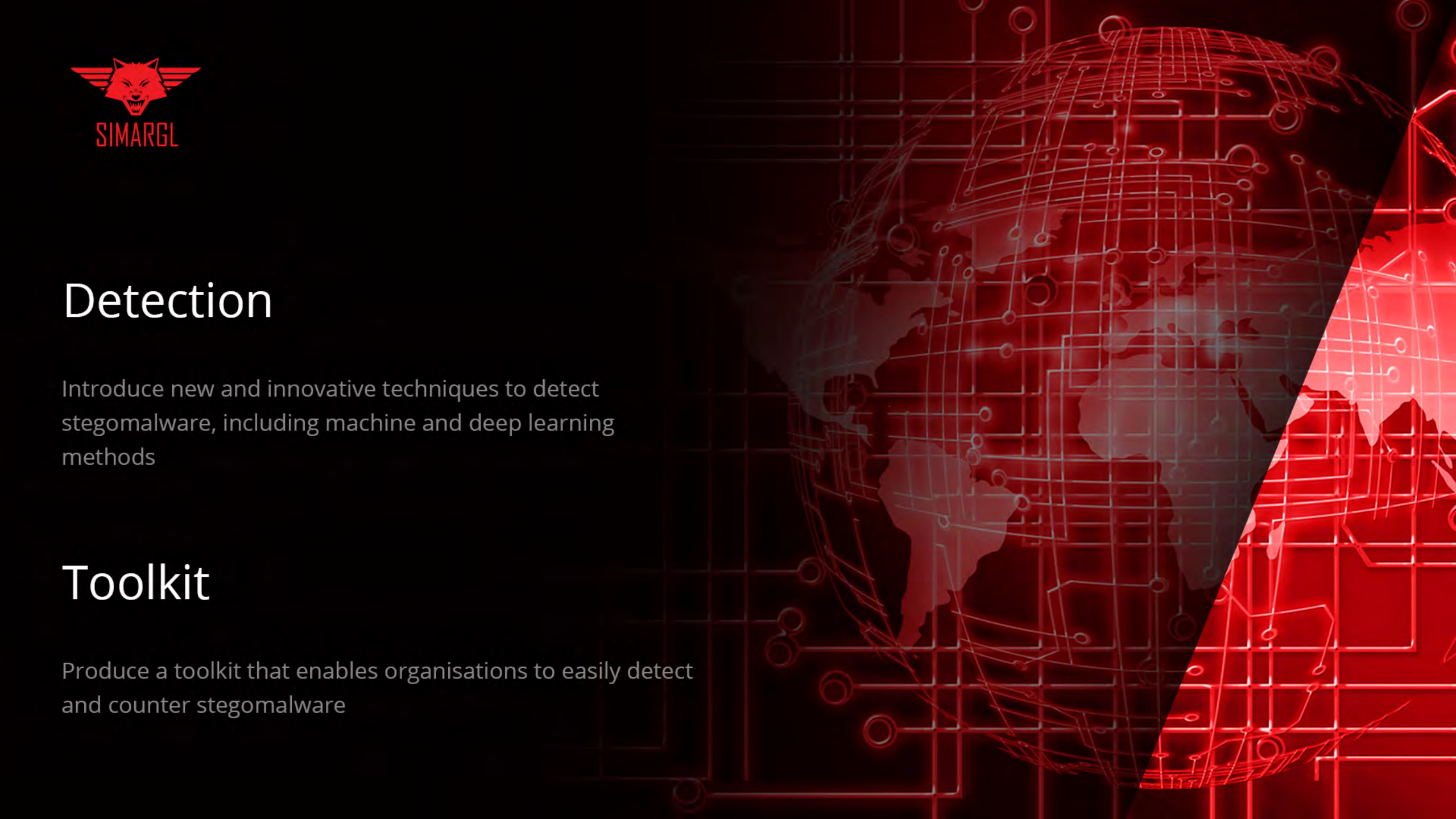
The Project

- SIMARGL will use breakthrough methods and algorithms to analyze the data from networks, such as:
  - concept drift detectors,
  - advanced signal processing and transformations,
  - lifelong learning intelligent systems (LLIS) approach,
  - hybrid classifiers, and
  - deep learning, just to mention some techniques.
- In the SIMARGL project 14 partners from 7 European countries unite their expertise and know-how

SIMARGL

The Consortium

- FernUniversität in Hagen (the coordinator, Germany)
- Netzfactor GmbH (Germany)
- Airbus CyberSecurity SAS (France)
- Thales SIX GTS France (France)
- Consiglio Nazionale delle Ricerche (Italy)
- NUMERA S.p.a. (Italy)
- Pluribus-One (Italy)
- Institute of International Relations (Czech Republic)
- ITTI Sp. z o.o. (Poland)
- Warsaw University of Technology (Poland)
- CERT Orange Polska (Poland)
- SIVECO Romania SA (Romania)
- RoEduNet (ARNIEC Agency) (Romania)
- Stichting CUIng Foundation (the Netherlands)

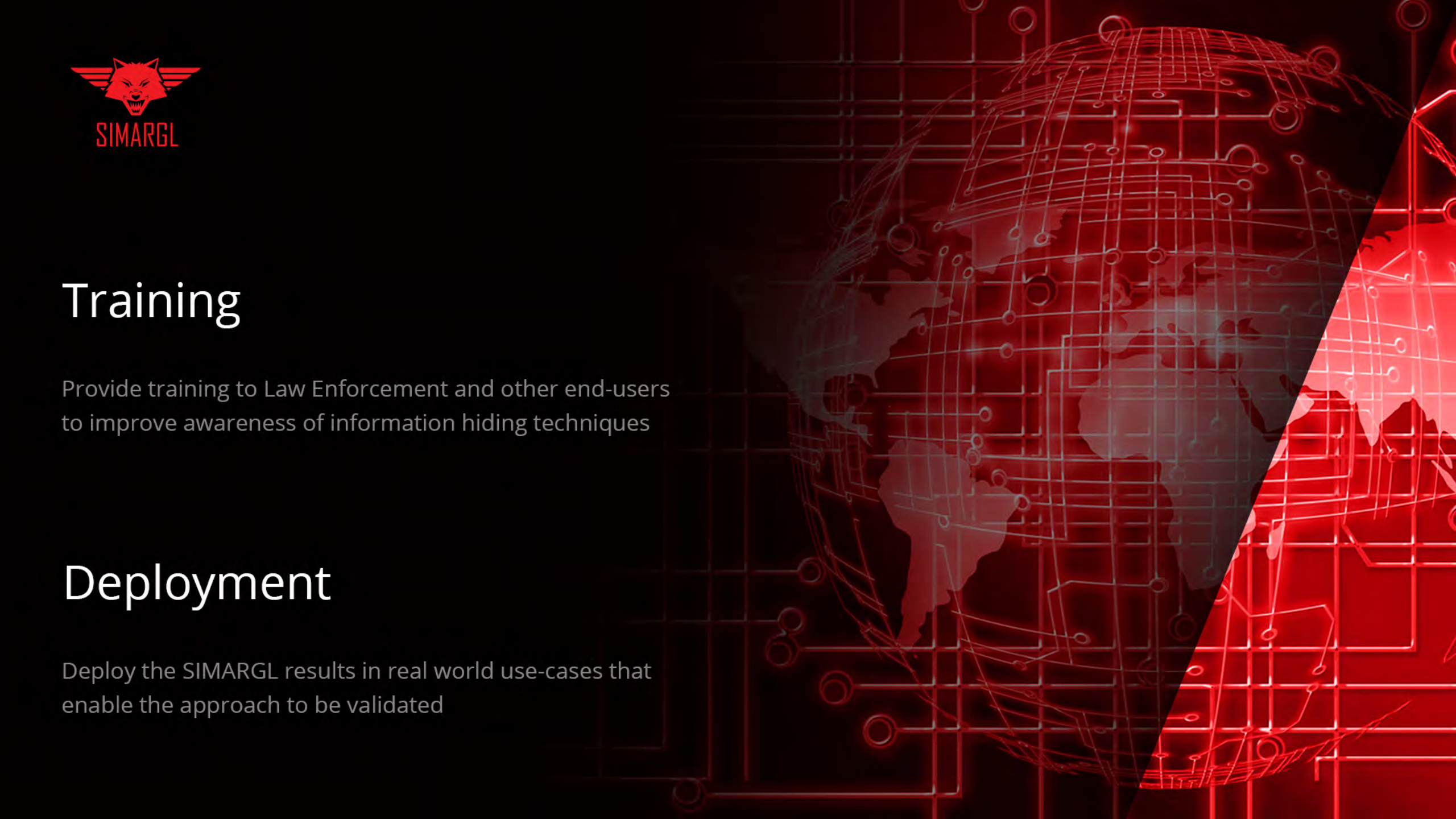


Detection

Introduce new and innovative techniques to detect stegomalware, including machine and deep learning methods

Toolkit

Produce a toolkit that enables organisations to easily detect and counter stegomalware



Training

Provide training to Law Enforcement and other end-users to improve awareness of information hiding techniques

Deployment

Deploy the SIMARGL results in real world use-cases that enable the approach to be validated

Contact and social media

- Website: https://simargl.eu/
- E-mail: contact@simargl.eu
- Follow us:
  - Facebook https://www.facebook.com/simargl.eu/
  - LinkedIn https://www.linkedin.com/groups/12241333/
  - Twitter https://twitter.com/SIMARGL8