



## **Wi-fi: MARRIOT\_CONFERENCE EVENT06**

# **cyberwatching.eu 2<sup>nd</sup> Concertation Meeting** ***#Concertation19***

04 June 2019  
*Brussels, Belgium*

[www.cyberwatching.eu](http://www.cyberwatching.eu) | [www.twitter.com/cyberwatchingeu](https://www.twitter.com/cyberwatchingeu)

cyberwatching.eu Concertation Meeting | Brussels, 04/06/2019

**Wi-fi: MARRIOT\_CONFERENCE**  
**EVENT06**

**Break-out 2: Standards and certification for  
cybersecurity**

Chair: Mark Miller, Conceptivity & ECSO Board of  
directors and Chair SWG1.3, WG1 Standards, certification

# Participants

## Break-out 2: Standards and certification for cybersecurity

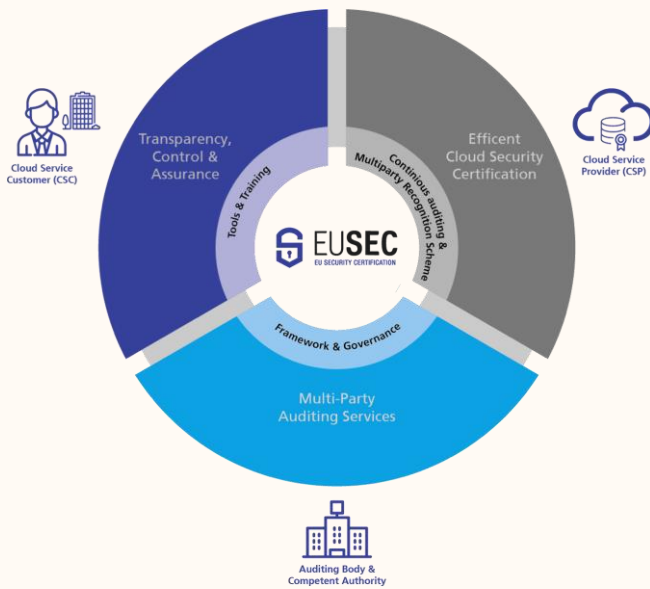
### Room 2

Chair: Sebastiano Tofaletti, Digital SME Alliance & Chair ECSO WG4 Support to SMEs

Name, Project/Organisation	Name, Project/Organisation
Abdelmalek Benzekri, CyberSec4Europe	Jürgen Großmann, EU-SEC
Claudio Caimi, C3ISP	Armand Puccetti, VESSEDIA
Nicolas Diaz, SPARTA	Eva Schlehahn, CANVAS & SPECIAL
Jos Dumortier, CyberSec4Europe	Sandra Strohbach, IMPACT
David Goodman, CyberSec4Europe	

# The European Security Certification Framework (EU-SEC)

Improve effectiveness and efficiency of existing cloud security certification schemes



- **Multiparty recognition framework** for cloud security certifications and
- **Continuous auditing based certifications**
- **Collect and maintain security and privacy requirements** relevant to the public and private sector.
- **Validate the framework with pilot use cases** executed by public and private sector partners to ensure its effectiveness, efficiency and market readiness in large scale demonstrators.
- **Strengthen the value proposition, market uptake and long-term sustainability** of EU-SEC framework through commercial exploitation, influencing other standardization initiatives and performing strategic awareness and training activities.
- **Develop a governance structure** to support trans-European EU-SEC framework adoption.



4th June 2019, Cyberwatching, Brussels

EU-SEC grant agreement no 731845



This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no. 731845.

# VESSEDIA Project Objectives, challenges & results for end users at M25

- ◆ **VESSEDIA** aims at enhancing the safety and security medium-criticality S/W, especially IoT. More precisely, making formal methods more accessible for application domains that want to improve the security and reliability of their software applications.
- ◆ **Results:**
  - ◆ 1) security requirements for IoT
  - ◆ Methodology for the V&V of IoT
  - ◆ 2) On-going use-cases analyses (Contiki, 6LowPAN, etc.) using C/C++/Java analysis tools
  - ◆ 3) Improved tools for the analysis of C/C++/Java: Frama-C and VeriFast
  - ◆ 4) Combined modelling & specification tools for vulnerabilities detection at source code level
  - ◆ 5) (on-going) draft of ISO standard for V&V tools
  - ◆ 6) Contributions to Common Criteria Certification process
  - ◆ 7) Metrics, security evaluations and quality tests of the tools.
  - ◆ 8) Common Workshop done with project CHARLOT in May 2019, Dublin.

Contact: Eva Schlehahn

Senior legal researcher and consultant at Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

uld67@datenschutzzentrum.de

**SPECIAL:** 

Technical specifications for GDPR-compliant data processing policies

➤ Data handling **policy enforcement and auditability**

**Standardization** of a taxonomy of privacy terms, esp. with regard to GDPR. Examples are taxonomies of:

- personal data categories,
- different data processing purposes,
- events of disclosures,
- consent status/modalities
- types of processing operations.

**Project website:**

<https://www.specialprivacy.eu/>

<https://www.w3.org/community/dpvcg>

**CANVAS:** 

Constructing an Alliance for Value-driven Cybersecurity

Informing stakeholders to address the challenge how cybersecurity can be aligned with European values and fundamental rights.

- **Briefing Packages**
  - Concise and comprehensive summaries of CANVAS results for policy makers
- **Reference Curriculum**
  - Integrating the value perspective into cybersecurity training and education
- **MOOC**
  - Massive Open Online Course
- **Upcoming: CANVAS Book**

**Project website:**

<https://canvas-project.eu/>



# imPACT —

PRIVACY, ACCOUNTABILITY, COMPLIANCE, AND TRUST IN TOMORROW'S INTERNET

Duration: February 2015 – January 2021

Funding volume: € 9,257,000

The solution for the security issues of tomorrow's internet:

- Protection of privacy, e.g., in social networks
- Accountability of users and providers
- Compliance of software and services with user expectations, applicable laws and provider policies
- Trustworthiness of information



Coordinator: Michael Backes, *Director CISPA*

Principal Investigators: Peter Druschel, *Founding Director Max Planck Institute for Software Systems*;  
Rupak Majumdar, *Scientific Director at the Max Planck Institute for Software Systems*;  
Gerhard Weikum, *Research Director at the Max-Planck Institute for Informatics*