ISAC FOR CITIES (I4C+)

"David against Goliath"

EU City Active | EU City Listener | EU No City Member | Non-EU City - Active | Non-EU City - Listener

An "ISAC for Cities" Special Interest Group (SIG) for Members of Major Cities Europe

Weekly "Coffee Meetings" on Friday morning 9.00 am CET – 10.00 am CET.

Monthly "Brown Bag" sessions (Usually second week of month Tuesdays 13.00 pm CET – 14.00 pm CET)

(Ad-Hoc) Collaboration on Expert Issues

Supported by EU Agency for Cybersecurity

Guided by EU Funded Project to Support ISACs

Protecting our Citizens by Reducing the Probability and Impact of Cyber-Attacks on our Cities and Regions

Sharing Knowledge

- Private Tips & Tricks
- Good practice
- Cyber-breaches and how they were resolved
- Cyber-solutions used and practical experiences
- Cyber-strategies and implementation experiences
- Benchmarking

Creating Intelligence

- Advisories & Notifications (w/ Multi State ISAC & MISP)
- Malicious Code Analysis (Aspired)
- Vulnerability Analysis (Aspired)

Resourcing Operations

- Collaboration Tools (w/ ISACs for EU Project)
- "Fingers and Thumbs" (Aspired)
- Shared 24x7x365 SOC (Aspired)

If you are CIO/CISO of a city please join us by sending your full contact details to i4cplus@majorcities.eu

Chair City ISAC I4C+ / Dr. Oliver Schwabe. Email: oliver.schwabe@isac4cities.eu.

Mobile: +49 (0) 1709053671. Web: https://i4c.isacs.eu/ & https://www.majorcities.eu/isac-for-cities-plus/

MAJOR CITIES OF EUROPE IT USERS GROUP

I4C+ is a decentralized Information and Analysis Centre (ISAC) whose members are CIOs/CISOs of EU cities (plus relevant aggregators) exchanging personal sensitive knowledge to improve their individual and collective cyber resilience. The "+" emphasize the "high touch, low tech" of our community. Community terms of reference available HERE. Community roadmap available HERE. I4C+ is a member of the European Cyber Security Community supporting Digital Europe.

The ISAC for Cities (I4C+) is a partner of the Empowering EU-ISACs project that has received funding from the European Commission's Directorate General CNECT under grant agreement number SMART2018/1022.

European Commission

Applied Research Study
"Increasing the Cyber Resilience of Critical IT Infrastructure Ecosystems in EU Public Administrations - Implementing the NIS2 Directive"
(Working Title: “DAVID”).

In January 2023, the OSEAN Research Group (https://osean.uma.pt/) at the University of Madeira (https://www.uma.pt/) led by Professor Eduardo Leite, Vice President at Higher School of Technology and Management, University of Madeira, is launching an applied research study focusing on "Increasing the Cyber Resilience of Critical IT Infrastructure Ecosystems in EU Public Administrations - Implementing the NIS2 Directive" (Working Title: “DAVID”) in collaboration with members of the EU City ISAC (https://i4c.isacs.eu/). This supports the “on the ground” implementation of the NIS2 Directive for local public administrations in Europe. All study materials are initially classified as [TLP:RED]. The study will initially run for 18 months and deliver:

1. A **Framework** for assessing current and desired NIS2 implementation maturity in and across critical infrastructure (Month 3).
2. A **Toolbox** for sustainably increasing implementation maturity (Month 6).
3. A Best Practice “Defence in Depth” **Guide** for collaborative improvement of cyber resilience (Month 9).
4. A **Blueprint** for a decentralized cyber security mesh across public administrations (Month 12).
5. A **Pilot** of the Blueprint in and across participating public administrations (Month 16 onwards).
6. A Joint-Defence **Agreement** among participating public administrations (Ongoing).
7. Related activities requested by study members as permitted by available funding, i.e. the establishment of a Threat Sharing MISP https://misp.isacs.eu/users/login) and the identification /capture of successful approaches for increasing funding / resources.