Automation SIG

2023 Annual Update

Version: 0.1 June 2nd, 2023

Chairs:
Aaron KAPLAN (Liaison)
Andreas MÜHLEMANN (SWITCH-CERT)
Benoît ROUSSILLE (EC Cybersecurity Operations Centre)
David DURVAUX (EC Cybersecurity Operations Centre)
Razvan GAVRILA (ENISA)
Vasileios MAVROEIDIS (UIO.no)
Vilius BENETIS (NRD CIRT)

About the Automation SIG

- Establish a **forum** for exchanging best practices in **Incident Response (IR) automation**.
- Develop a comprehensive **best practices document** for automation in IR.
- Create a curated list of **automation tools** for IR and their specific focus areas.

- Details & SIG bylaws: **https://www.first.org/global/sigs/automation**

Activities

- Monthly SIG calls
- Presentations of Automation tools, standards (CACAO, …), SOARs, etc.

- Initial Best Common Practices Document: https://stage.first.org/global/sigs/automation/bcp-guide/

- Development model: github (develop, stage, main- branches)
- Solid template for describing use-cases and tools (thx to Braxton)
- Beta-Release of the BCP guide.
- Survey coming (thx to Razvan): which tools are in use in Automation?

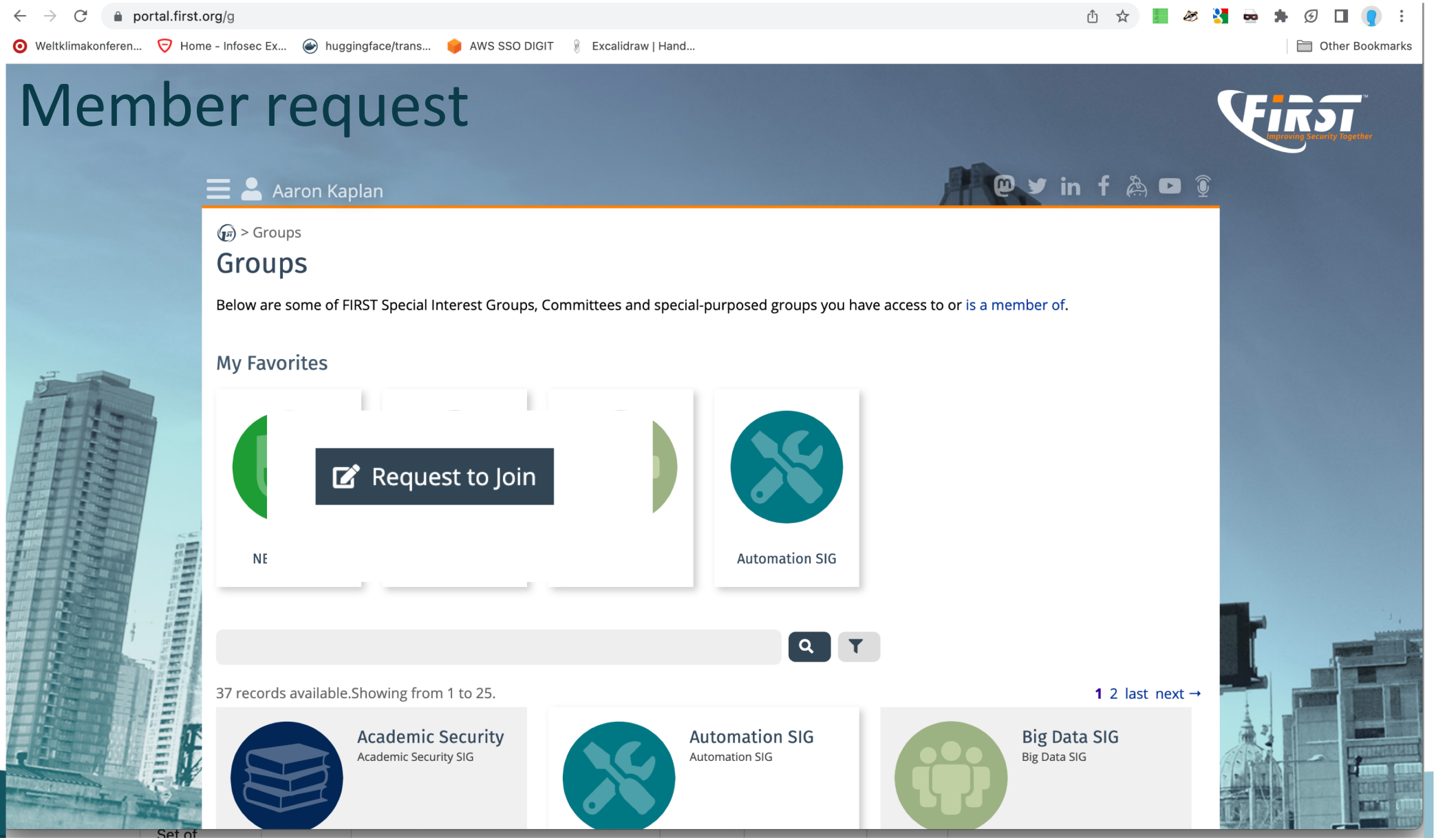
Membership (status)

- **Audience:**
  Anyone interested in IR Automation

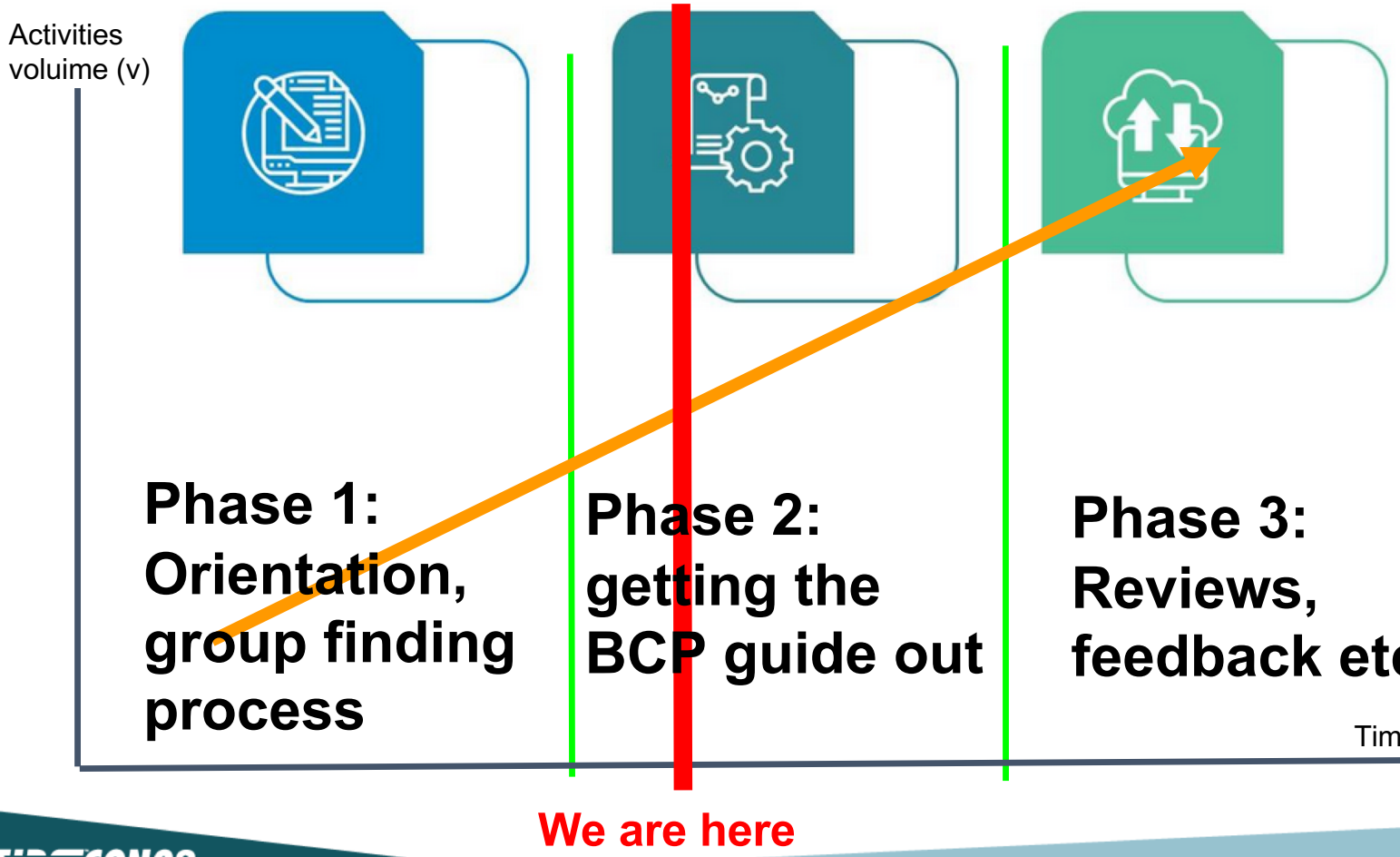
- **Current membership:**

  82 members

- **Requirements:**
  - Dedicate some time to participate, add your use-cases and tools


portal.first.org/g
Weltklimakonferen...
Home - Infosec Ex...
huggingface/trans...
AWS SSO DIGIT
Excalidraw | Hand...
Other Bookmarks
Member request
Aaron Kaplan
> Groups
Groups
Below are some of FIRST Special Interest Groups, Committees and special-purposed groups you have access to or is a member of.
My Favorites
Request to Join
Automation SIG
37 records available.Showing from 1 to 25.
1 2 last next →
Academic Security
Academic Security SIG
Automation SIG
Automation SIG
Big Data SIG
Big Data SIG

Automation SIG Activity's Progress Roadmap



Thank you!

Contact us:

Slack #automation-sig ←

www.first.org/global/sigs/automation/