CINCAN

Codifying your malware/artifact analysis workflows

or, Building shareable, repeatable & history preserving analysis pipelines using your favourite tools + git + containers

Co-financed by the Connecting Europe Facility of the European Union

UNIVERSITY OF OULU

TRAFICOM

jamk.fi

Motivation (user point of view)

Enlightenment by listening to rants from analysts

- Solving fragility - tools don’t always work in every env & every time
- Teaching and sharing* the workflow
- Making the workflow repeatable
- Automating stuff
- Sharing* results
  - repeatability & transparency

*Both within team & with collaborators or maybe even the world (open-source)

Co-financed by the Connecting Europe Facility of the European Union

Motivation (developer POV)

Riding the big productivity & collaboration tech trends

- “Githubification of infosec” - leverage technologies like Github/Gitlab, Docker containers, CI/CD, collaborative ways of working
- Once a tool packaged in a container, it can be very easily integrated into different environments & systems - solve packaging & deployment
- Automation
  - Credibility & robustness of results by verifiability & repeatability & transparency
  - Continuous testing of changes & continuous proof of “it’s still working”

Co-financed by the Connecting Europe Facility of the European Union

UNIVERSITY OF OULU TRAFICOM jamk.fi

Background

EU funded project, ending in 6/2020

- Original schedule 2018-2019, extended to 2020-06
- Parties
  - National Cybersecurity Center (in Finnish Transport and Communications Agency)
  - Oulu University Secure Programming Group
  - JAMK University of Applienced Sciences
  - Funding from EU's INEA agency, from CEF program (Connecting Europe Facility)
  - You (users / collaborators) - open source project!

Co-financed by the Connecting Europe Facility of the European Union

UNIVERSITY OF OULU TRAFICOM jamk.fi

CinCan products you can use now

Tools and packaging work

- Many DFIR tools packaged for docker (see https://gitlab.com/CinCan/tools/) and ready to run
- open source cli tool “cincan” available to easily run DFIR tools and handle data input/output
  - `cincan run cincan/apktool d samples/selendroid-test-app.apk -o samples/cincanTest`
- Many blog posts about how to use these tools (https://cincan.io/blog/)

Co-financed by the Connecting Europe Facility of the European Union

UNIVERSITY OF OULU TRAFICOM jamk.fi

CinCan products you can use now

Other products

- CI/CD based workflow automation solution
  - Automatically run pipeline of tools when new input data appears in Gitlab
  - Uses CinCan packaged tools & Concourse CI system & Gitlab
- open source cli tool “minion”
  - rule based multi step workflows, and example rulesets

Co-financed by the Connecting Europe Facility of the European Union

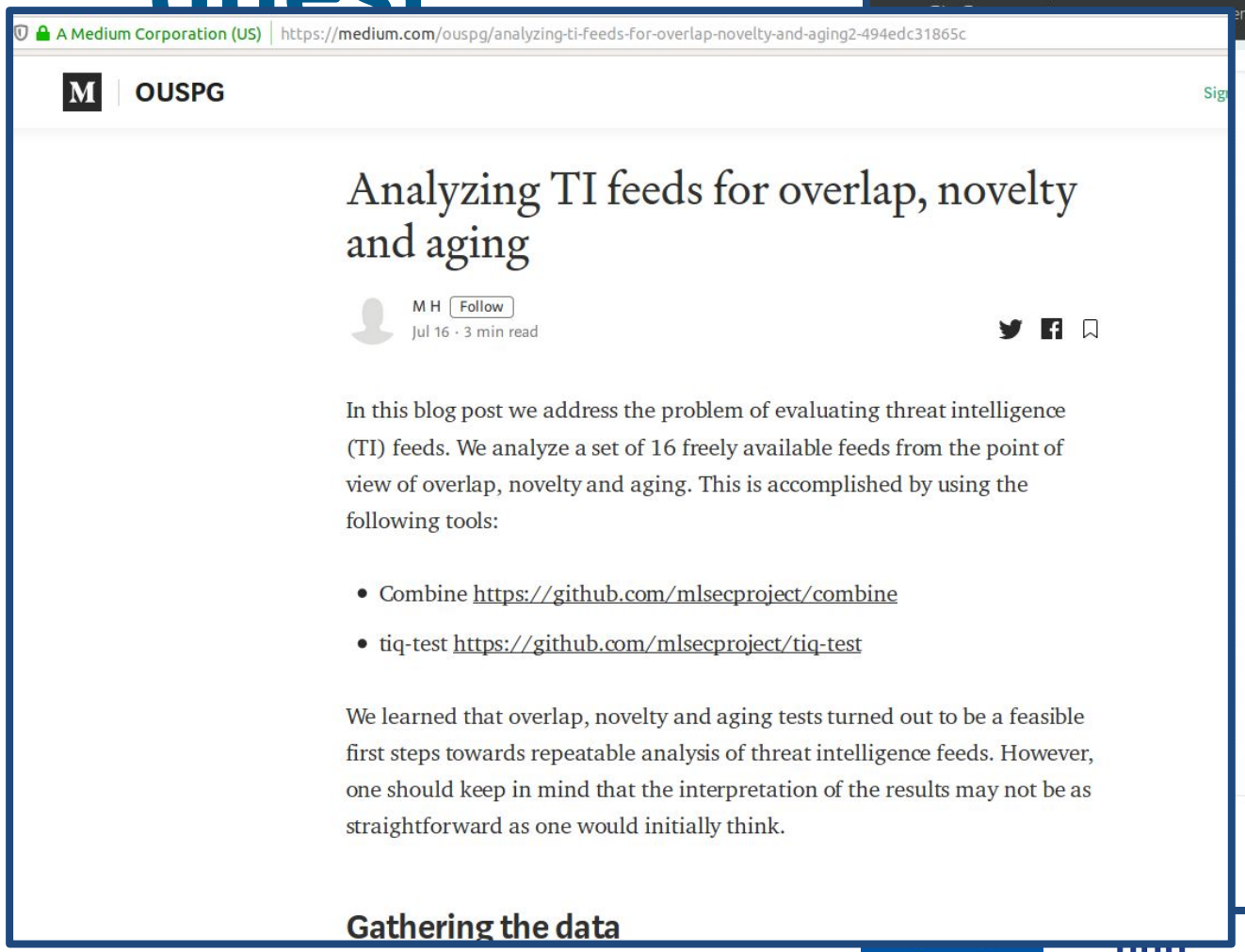
PILOTING

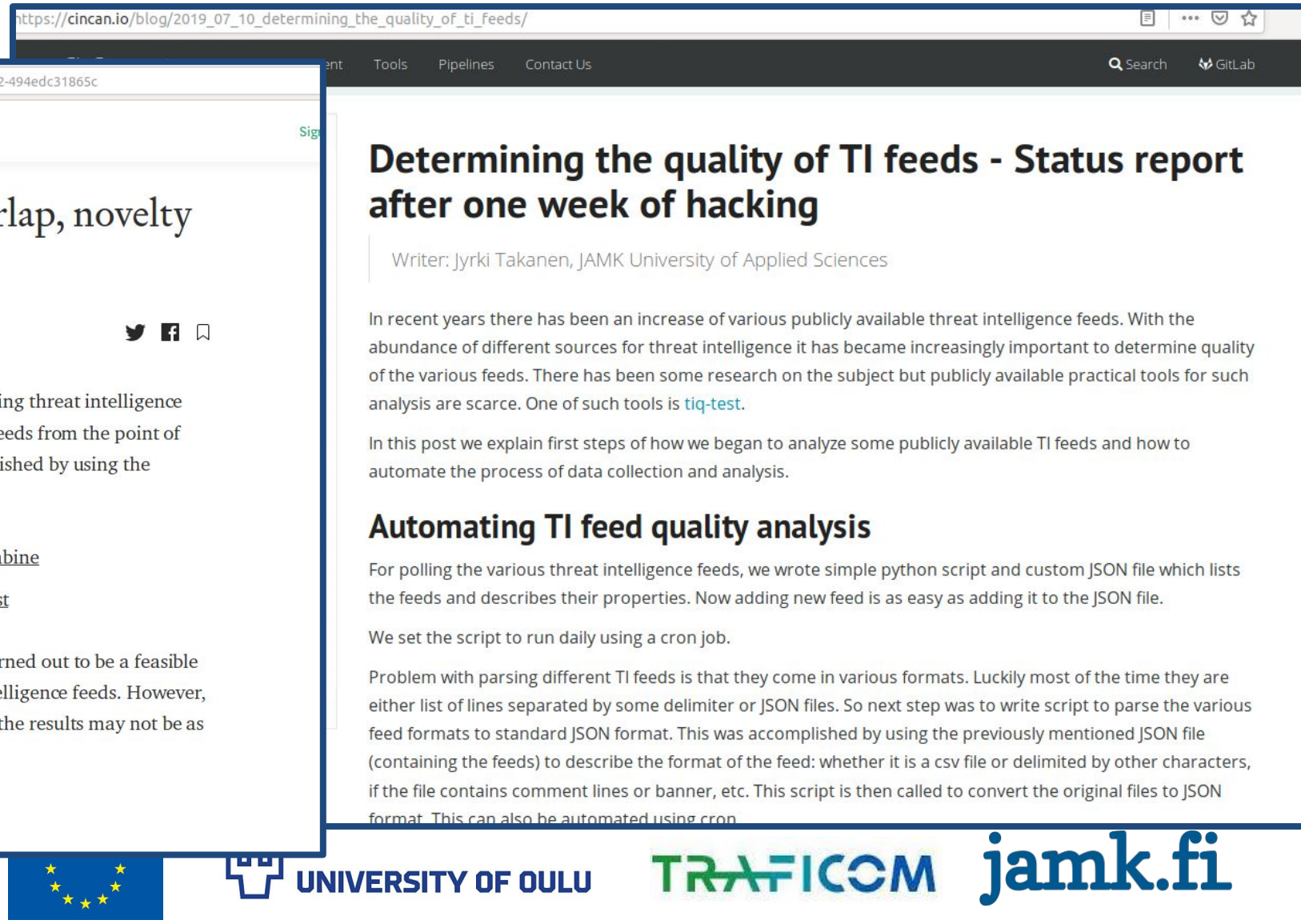
European CERTs wanted, but also SoCs etc

- We want as many users as possible
- Sign up, hear our 20 minute intro / pitch, try out some of our tools & give us feedback!

UNIVERSITY OF OULU TRAFICOM jamk.fi

Quality of Threat Intelligence side quest





UNIVERSITY OF OULU
TRAFICOM
jamk.fi

TO FOLLOW/JOIN THE PROJECT

- https://gitlab.com/cincan
- https://cincan.io
- Twitter: @CinCanProject

- email contact cincan@traficom.fi

Co-financed by the Connecting Europe Facility of the European Union