CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

DDoS Clearing House for Europe (Task 3.2) Status Update GA5

Cristian Hesselman
(SIDN Labs)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Result review #2, Sep 22, 2020

- “The project has made a good progress concerning the threat intelligence sharing and the DDoS clearing house platforms”

- “There is a fair bit of activity in clearing houses and threat sharing platforms globally in all sectors. […] ensure Concordia is not inventing the wheel […] The reviewers can facilitate introductions with the Multistate ISAC and Centre for Internet Security."

- **Follow-up action T3.2**: learn how Multistate ISAC works (in NL, ISACs are sector-specific and focus on people sharing info, which is unlike T3.2’s focus on cross-sector and services for better info sharing)

T3.2 Status

- Agreed overall architecture
- Prototypes of several components, at different maturity levels
- Agreed partner responsibilities and demo-driven way of working
- Active collaboration: in T3.2, with T3.1 and NL pilot partners
- Future challenge: interaction with production systems

T3.2 objective

- Pilot a DDoS Clearing House with European industry for Europe to proactively and collaboratively protect European critical infrastructure against DDoS attacks

- Contributes to **increased European digital sovereignty** thru better insight in and control over DDoS attacks

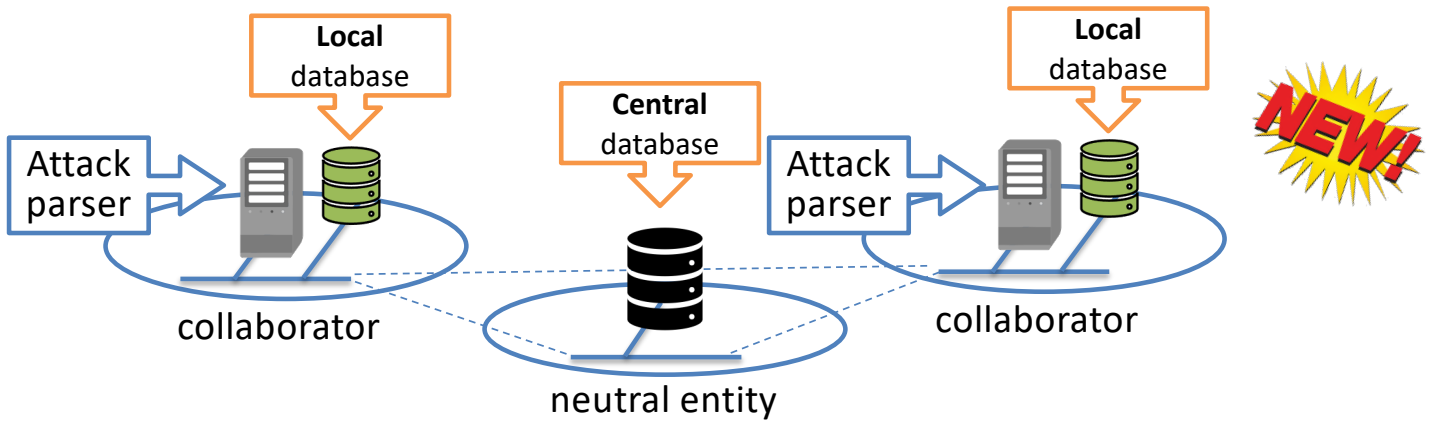
Key challenge: increase to TRL 5-7 and grow deployment

- Key outputs: **pilots** in NL >> IT, DDoS clearing house **blueprint**

DDoS Clearing House Concept

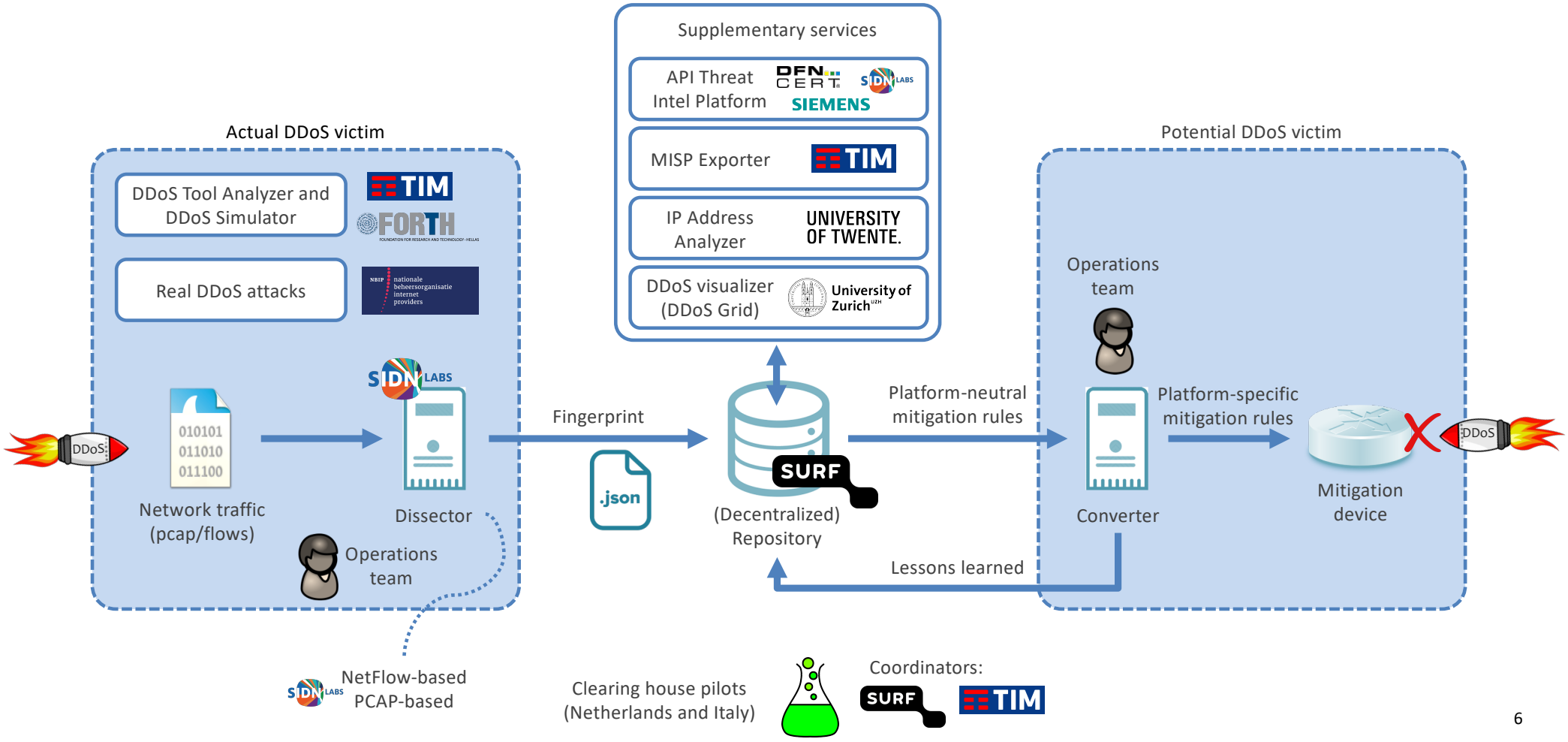
- Continuous and automatic sharing of “DDoS fingerprints” buys providers time (proactive)

- Extends DDoS protection services that critical service providers use and does not replace them



Based on presentation 2nd CONCORDIA review, Sep 22, 2020
This version: Oct 23, 2020

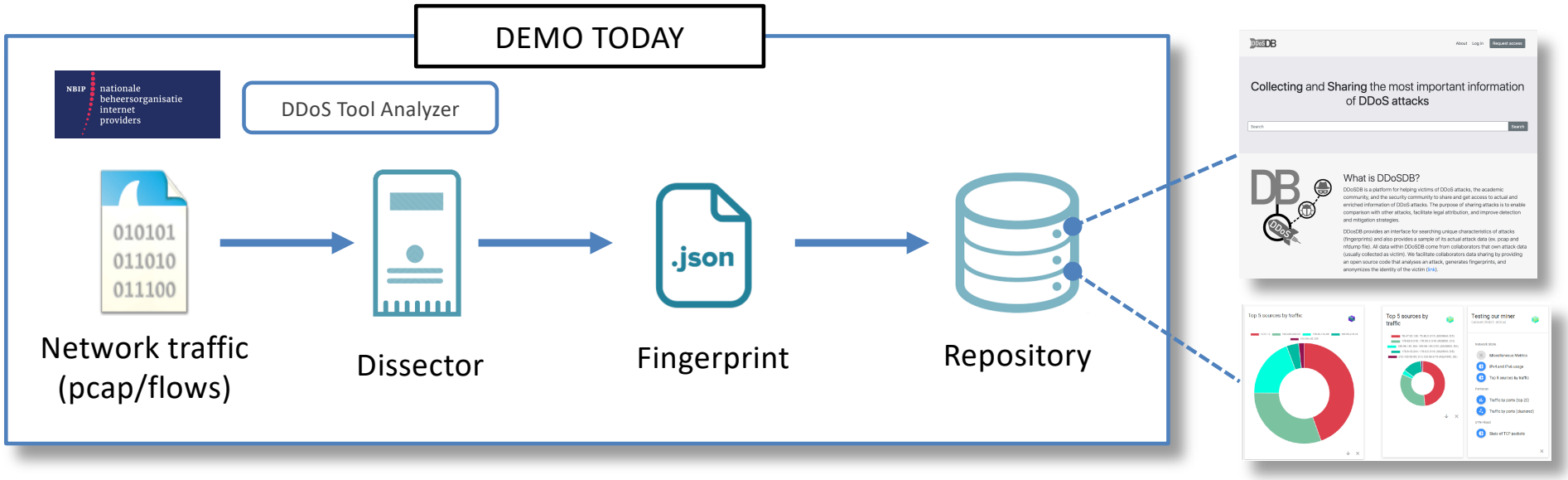
Main Components and Data Flow



Component Maturity Indication

Name	Function	Maturity	T3.2 experts (owner)
Dissector	Generate DDoS fingerprints based on PCAP files and flows data	High	João
DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High	Remco, João
Converter	Generate mitigation rules based on DDoS fingerprints	Low	João, Marco, Paolo
DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High	Bruno, Muriel
IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack, based on measurements	Low	Ramin, Mattijs
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks	Low	Christos
MISP Exporter	Generate MISP events based on DDoS fingerprints	Low	Madalina, Marco
Synthetic traffic generator	Generation of DDoS fingerprints using a TIM's DDoS traffic simulator	Low	Paolo

Today's Demo

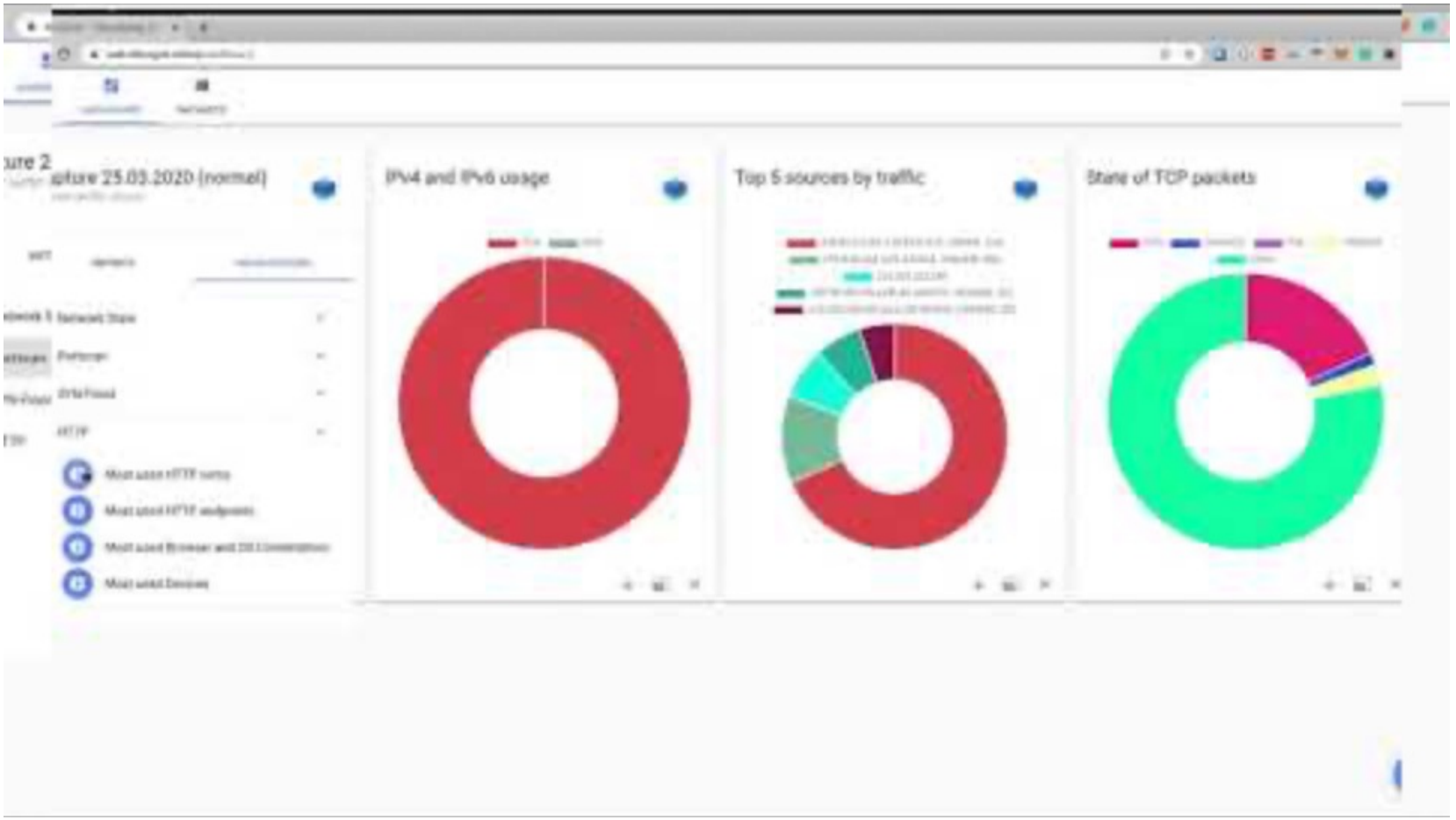


1. Full cycle process (generation, upload, storage)
2. Dashboard for fingerprint visualization
3. Fingerprint enrichment
4. DDoS Tool Analyzer automatically uploads fingerprints

Fingerprint generation, storage, enrichment

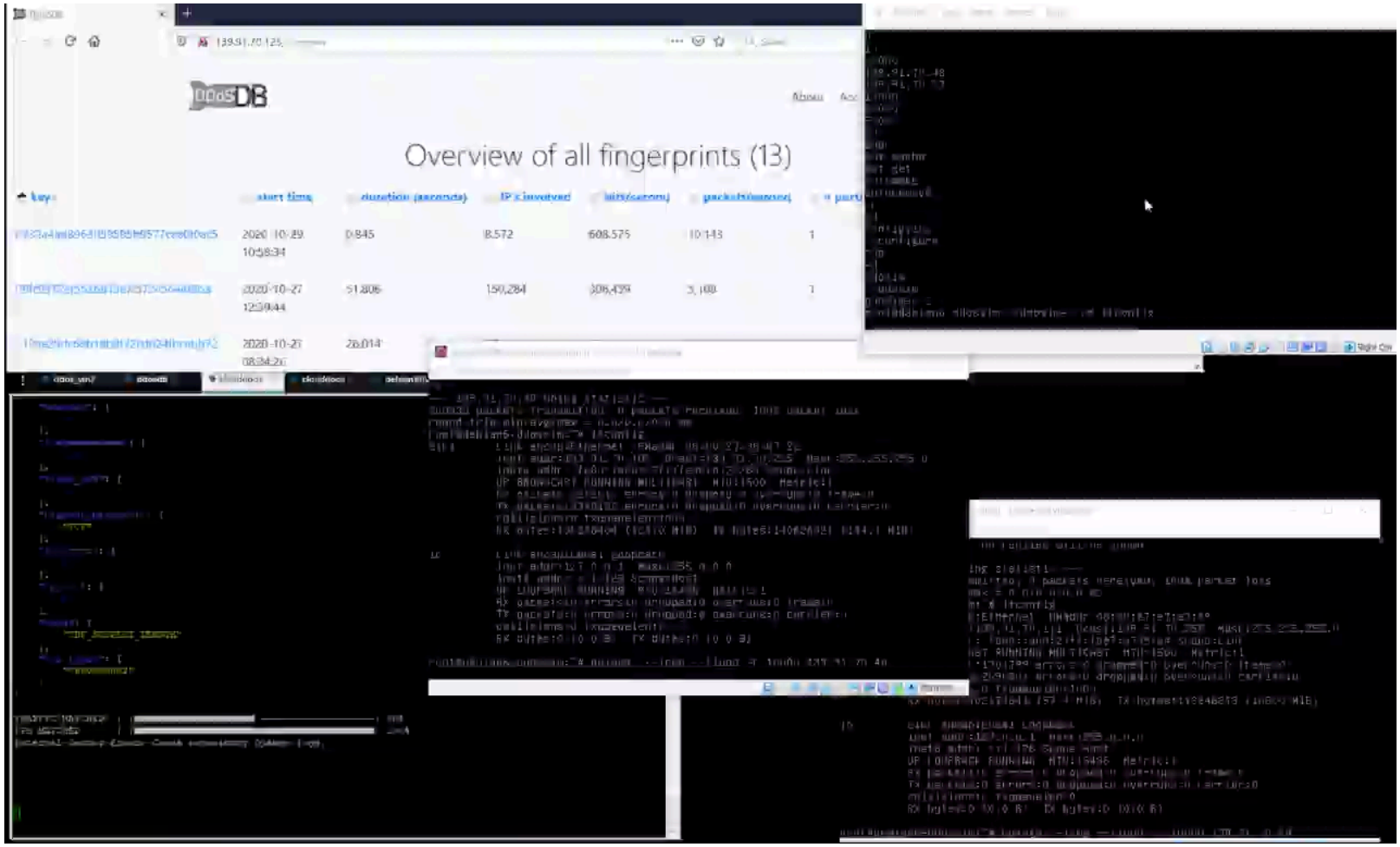
https://www.youtube.com/watch?feature=oembed&v=1QlC3SwwYAU

Fingerprint visualization (not integrated yet)



https://www.youtube.com/watch?feature=oembed&v=5OiCStFuerg

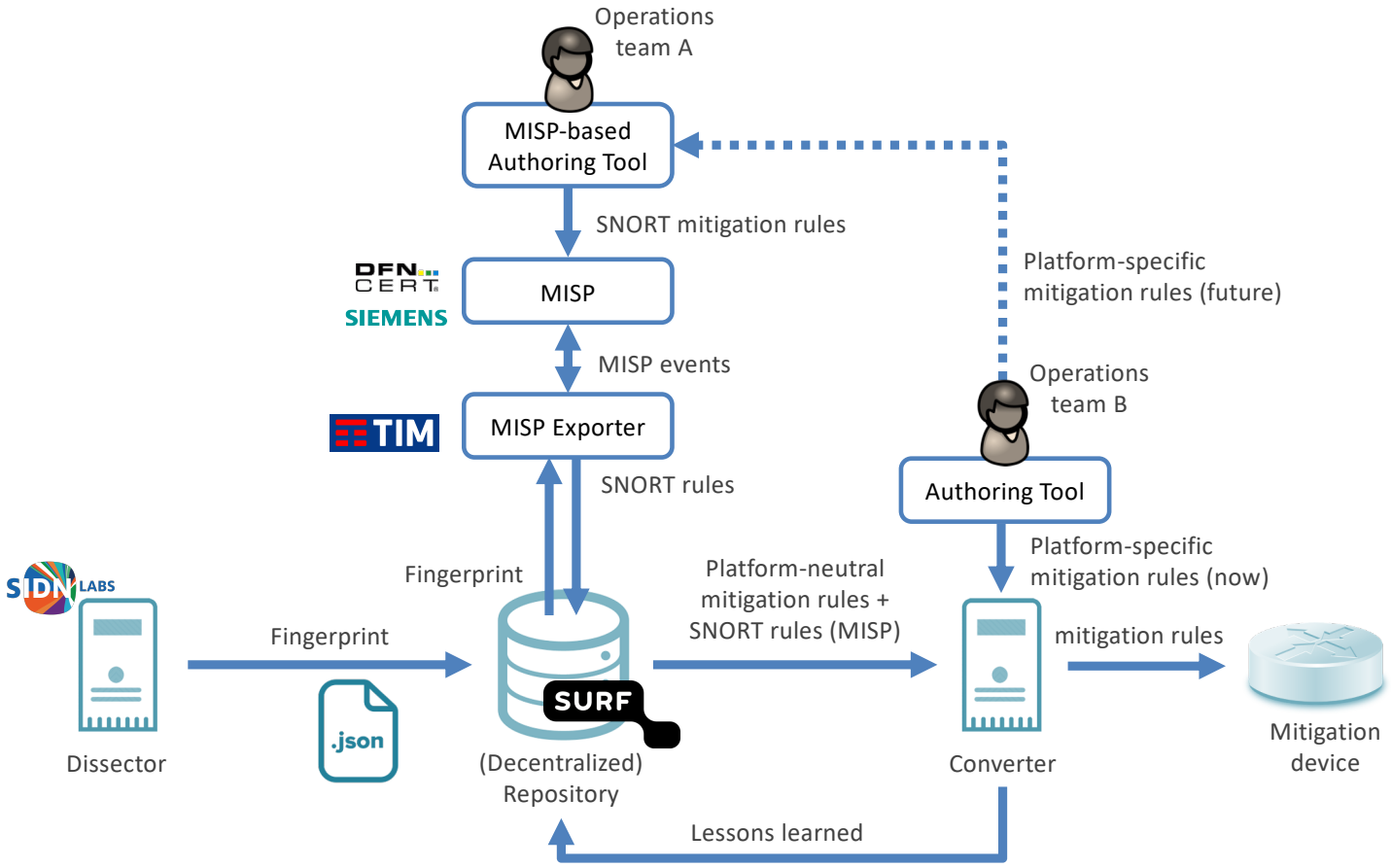
DDoS Tool Analyzer (not integrated yet)



Demo v2.3 (Dec 31, 2020)

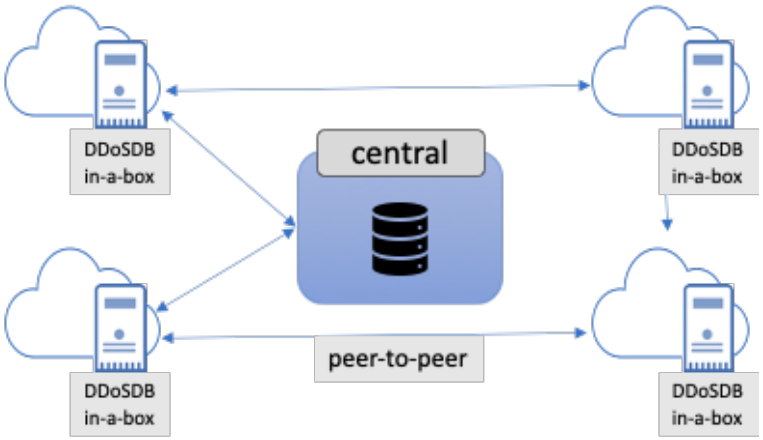
Name	Objective
Dissector	Dissector provides better APIs to other components (P2P communication, interface to supplementary services)
DDoSDB	DDoSDB provides APIs for DDoS Grid and other supplementary services.
Converter	Converter uses a MISP module to convert DDoS fingerprints from DDoSDB into mitigation rules (to be discussed on Oct 9)
DDoS Grid	Grid supports new kinds of fingerprint visualization, interworks with DDoSDB to add/get fingerprints
IP Address Analyzer	Analyzer reads fingerprints from DDoSDB, adds metadata based on measurements (e.g., host's network capacity and connection type), writes back to DDoSDB
DDoS Tool Analyzer	Profiler automatically and continually profiles DDoS tools and automatically uploads fingerprints to DDoS-DB
MISP Exporter	Exporter takes a fingerprint from DDoSDB and injects it into MISP as a MISP event. Detailed scenario description), based on Sep 2020 blog
Synthetic traffic generator	To be provided by mid Nov

MISP Interaction (work in progress)



Next steps

- Advance clearing house pilot in NL
- Improve and integrate components
- DDoS clearing house long-term roadmap
- Continue demo-driven approach
- Short term: contribute to D3.2 (M24)



Further reading

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

Dutch Anti-DDoS Coalition:
https://www.nomoreddos.org/en/

Clearing house on GitHub:
https://github.com/ddos-clearing-house/

Cristian Hesselman (T3.2 lead)
cristian.hesselman@sidn.nl
@hesselma
+31 6 25 07 87 33

This work was funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/