



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

Cristian Hesselman
(SIDN Labs)





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

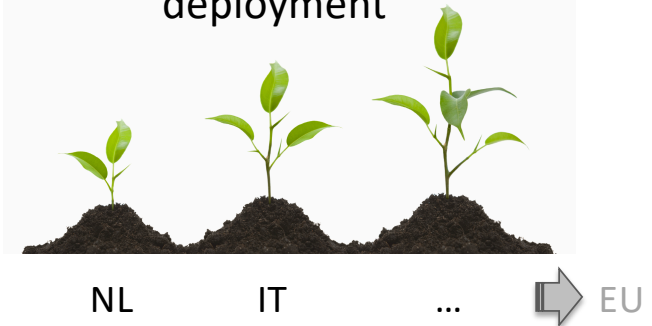


T3.2 objective

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



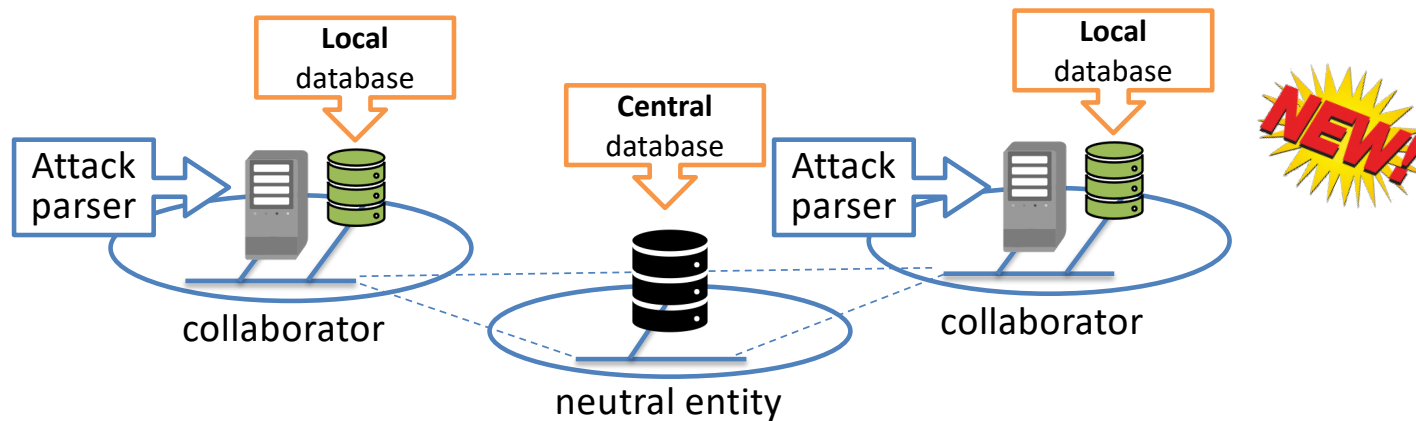
Key challenge: increase to
TRL 5-7 and grow
deployment





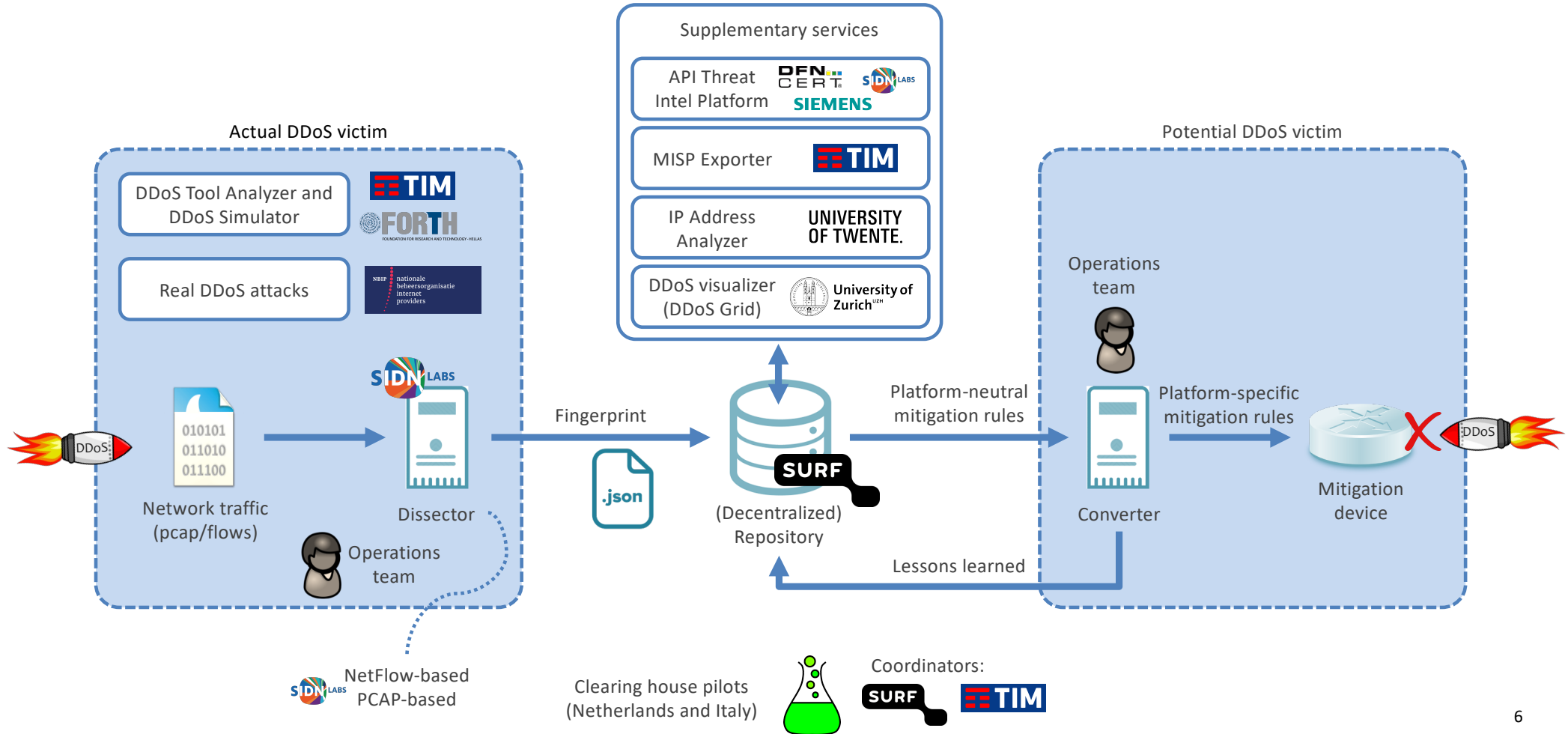
DDoS Clearing House Concept

- 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





Main Components and Data Flow



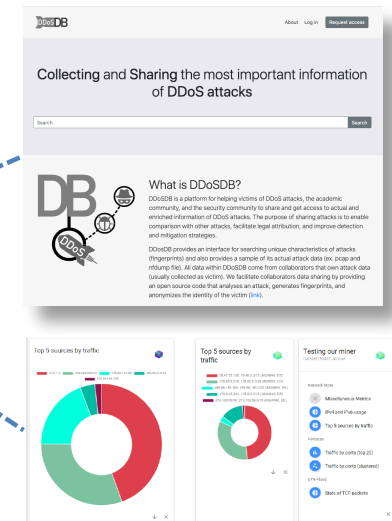
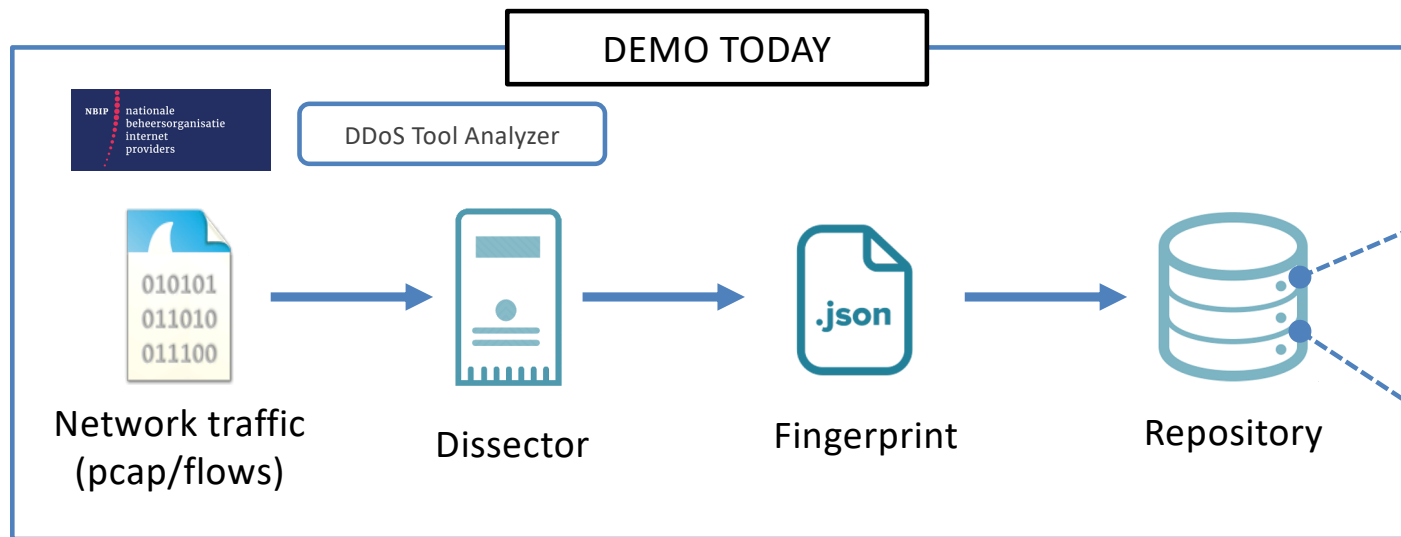


Component Maturity Indication

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



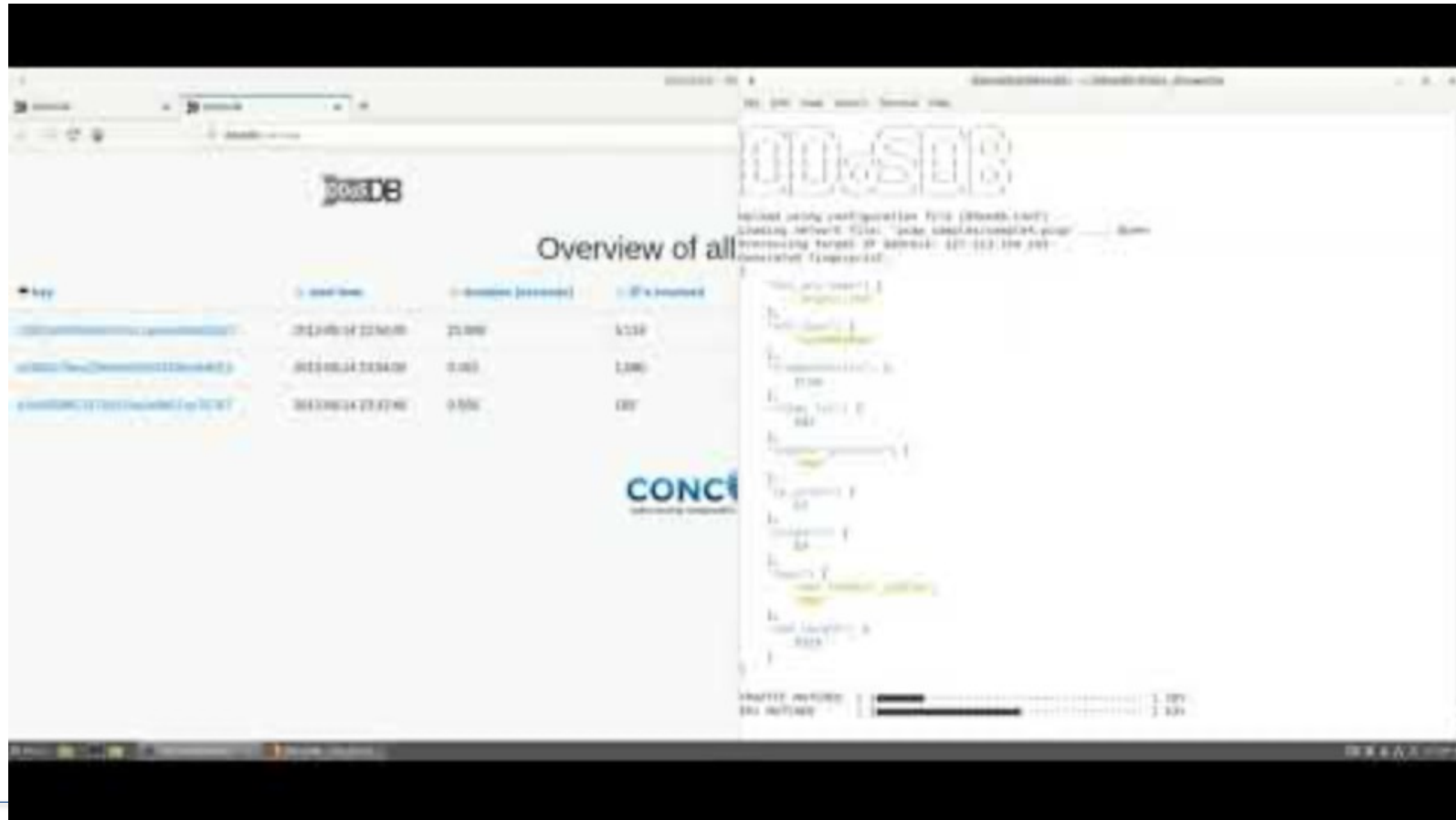
Today's Demo



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

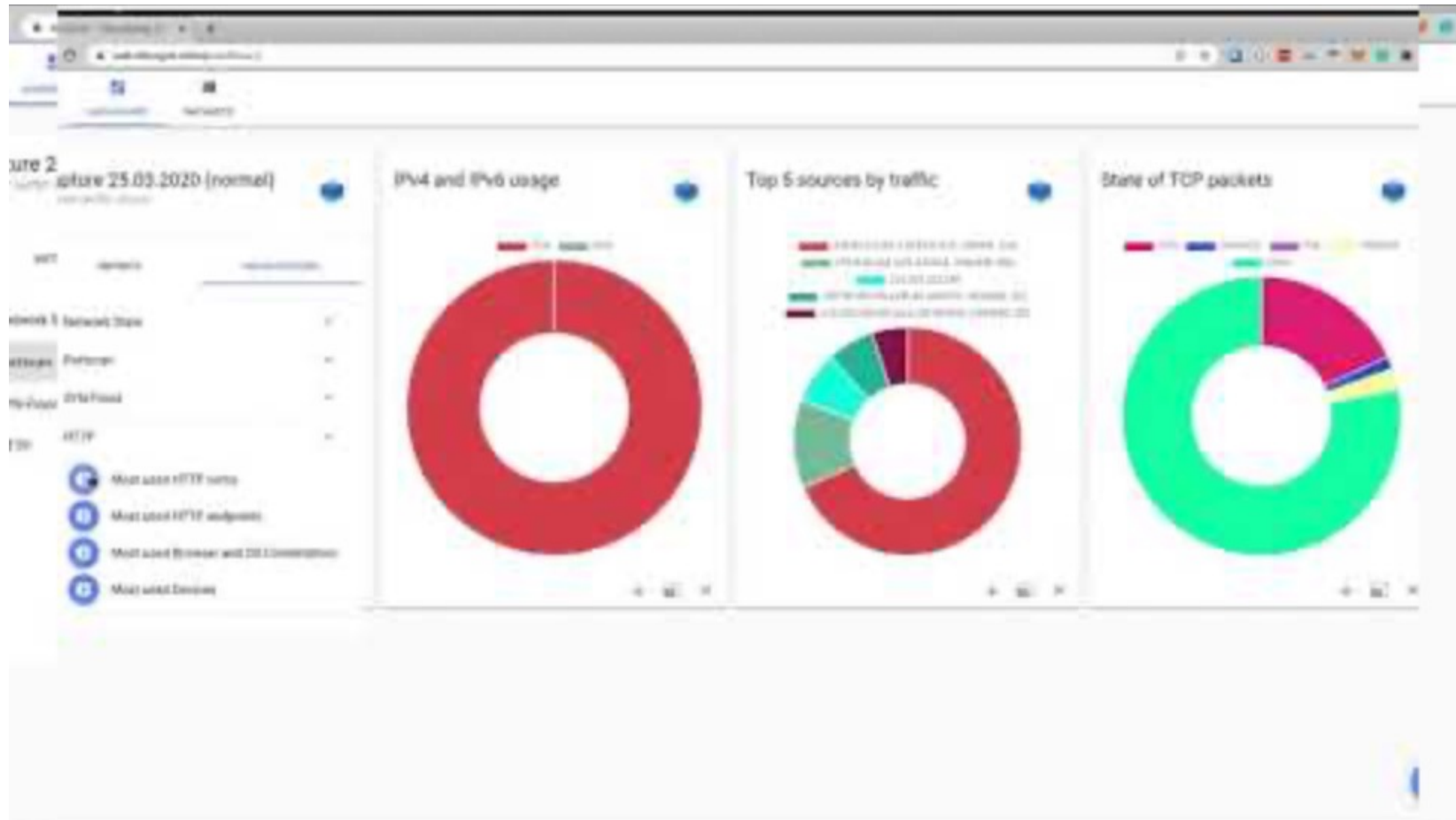


Fingerprint generation, storage, enrichment





Fingerprint visualization (not integrated yet)



<https://www.youtube.com/watch?feature=oembed&v=50iCStFuerg>



DDoS Tool Analyzer (not integrated yet)

The screenshot displays the 'Overview of all fingerprints (13)' page in the DDoS DB application. The page features a table with the following columns: 'key', 'start time', 'duration (seconds)', 'IPs involved', 'hits/seconds', 'packets/seconds', and 'ports'. Three entries are visible in the table:

| key | start time | duration (seconds) | IPs involved | hits/seconds | packets/seconds | ports |
|--|---------------------|--------------------|--------------|--------------|-----------------|-------|
| 193.4.118.80:68119:8584:69577:core01:ov5 | 2020-10-29 10:58:34 | 0.845 | 8,572 | 608,575 | 10,143 | 1 |
| 193.4.118.80:68119:8584:69577:core01:ov5 | 2020-10-27 12:09:44 | 51,806 | 159,284 | 306,439 | 3,100 | 1 |
| 193.4.118.80:68119:8584:69577:core01:ov5 | 2020-10-25 08:34:21 | 26,014 | | | | |

Below the table, there are several terminal windows showing network traffic analysis. One terminal window displays a list of IP addresses and their associated traffic statistics, such as 'IP: 193.4.118.80' and 'IP: 193.4.118.81'. Another terminal window shows a detailed view of a specific IP address, including its IP address, start time, duration, and traffic statistics.

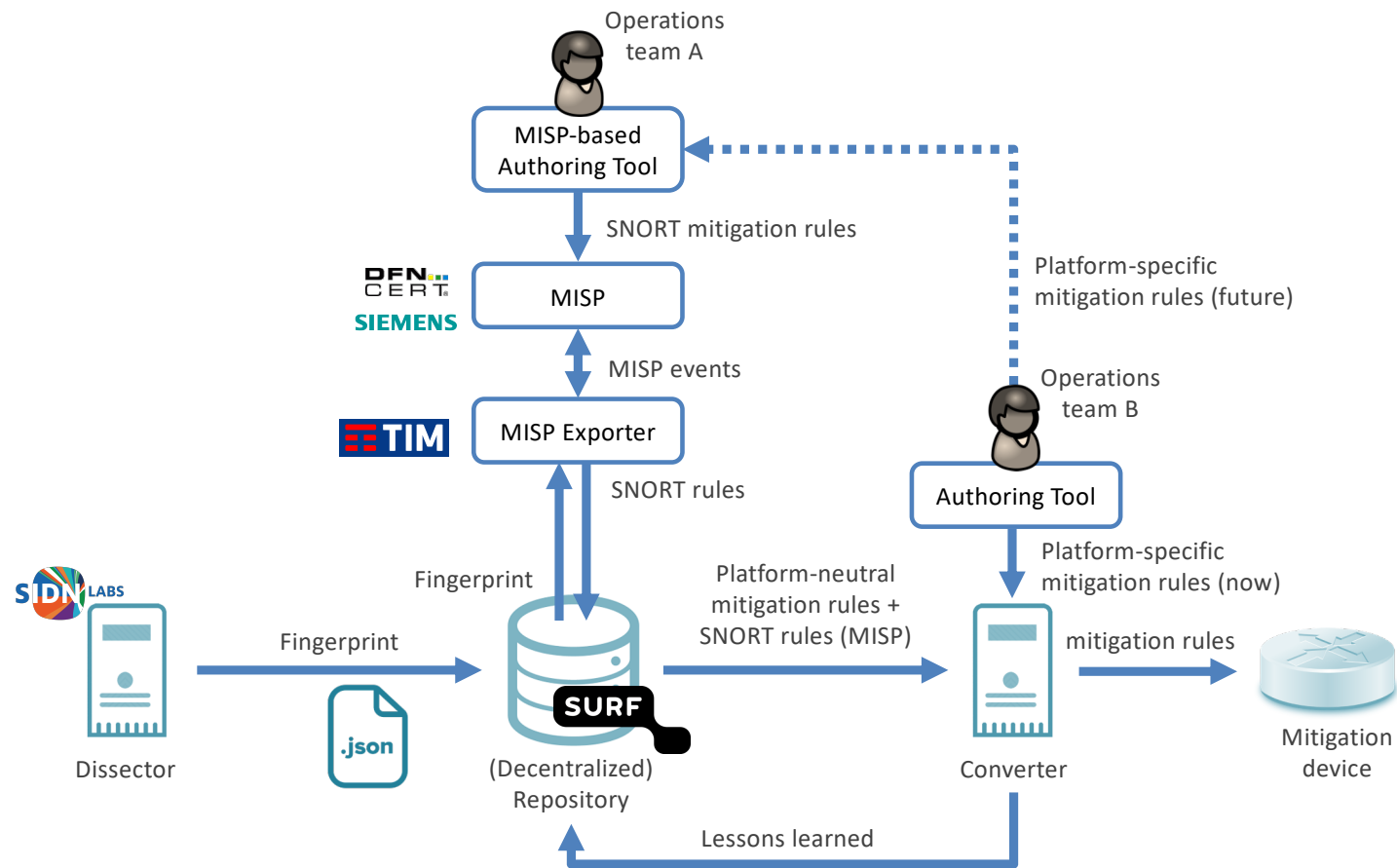


Demo v2.3 (Dec 31, 2020)

| 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 |



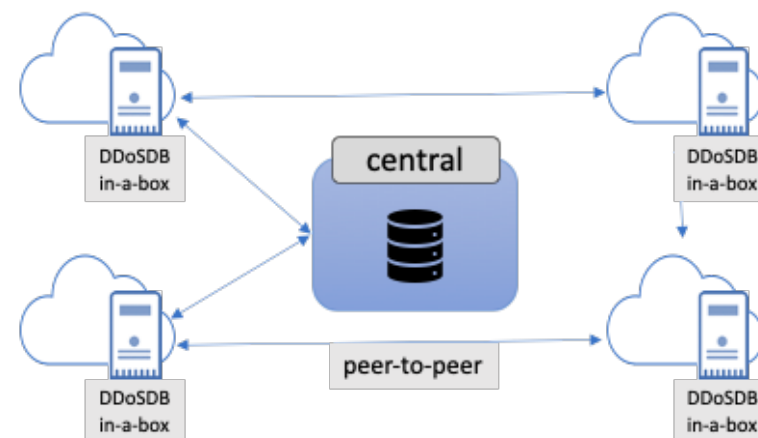
MISP Interaction (work in progress)





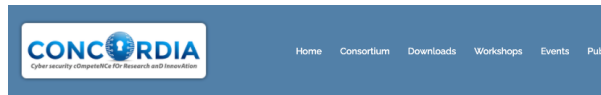
Next steps

- 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



POSTED APRIL 9, 2020 ADMIN CONCORDIA

Increasing the Netherlands' DDoS resilience together

First lessons learned from setting up a national anti-DDoS initiative, part I of III

The Dutch Anti-DDoS Coalition is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, government agencies and law enforcement) committed to fighting DDoS attacks together. In this series of three blogs, we'll first discuss the rationale behind our initiative, then describe a technical facility called the DDoS clearing house that enables coalition members to automatically measure and share the properties of DDoS attacks (e.g. attack duration and source IP addresses), before finally reviewing our key challenges, the lessons learned and the way forward. Our lessons learned are an important input for a "cookbook" to set up anti-DDoS coalitions elsewhere in Europe.

Note: we're using two types of reference in this blog series: hyperlinks refer to information, while numbers between straight brackets ([1]) link to in-depth technical papers.

DDoS attack landscape

A Distributed Denial-of-Service (DDoS) attack overwhelms a network with traffic, thus denuding the network's ability to service legitimate requests from their clients. The attacker typically does this by simultaneously transmitting traffic from a large number of machines distributed across the Internet, often by infecting those machines with malware that carries out the attack. Another type of attack is when an attacker exhausts a server's resources (rather than swamping the network) by repeatedly starting a login session with the server, thus forcing it to make more connections than it can handle.



New version of the DDoS Clearing House core components

The next round of improvements to get it deployed

Geplubliceerd op: donderdag 17 september 2020

SIDN Labs and SURF have released a new version of the DDoS Clearing House in a Box, a system that enables network operators to automatically share details of the DDoS attacks they handle, in the form of 'DDoS fingerprints'. In this blog, we briefly outline our improvements and how they contribute to the trials we'll be carrying out in the Netherlands and Italy.

Anti-DDoS Coalition and CONCORDIA

SIDN and SURF are proud to be part of the Dutch Anti-DDoS Coalition as well as of the CONCORDIA project, where we work on mechanisms and tools that enable service providers to handle DDoS attacks more proactively. Both projects involve numerous organisations including governments, internet providers, internet exchanges, academic institutions, non-profit organisations and banks.

An important building block in both projects is the DDoS Clearing House, a shared system that enables participating service providers to automatically share the characteristics of DDoS attacks they handle in the form of so-called 'DDoS fingerprints'. The tenet here is that to be forewarned is to be forearmed. Sharing DDoS fingerprints with other participants warns them that new attacks may be underway and extends the DDoS mitigation services that participants already have in place, such as scrubbing services like the [hulks](#). Comparing attacks currently in progress with attacks whose details are already recorded in the Clearing House can also provide pointers as to the best way to mitigate ongoing attacks.

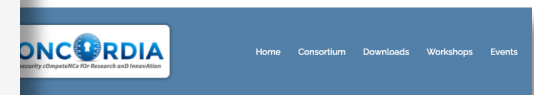
Recent [developments](#) show that DDoS attacks are still very much an issue and - more worryingly - are increasing in size, making our work with the DDoS Clearing House all the more relevant and pressing.



Jojo Ceron
Research engineer
[@jojoceeron](#)



Remco Poortinga-van Wijnen
Team Lead Security @ SURF
[remco@surf.nl](#)



SEPTEMBER 24, 2020 ADMIN CONCORDIA

Work in Progress: the CONCORDIA Platform for Threat Intelligence

First steps to improve Europe's information position in cybersecurity

Present CONCORDIA's vision for a cross-sector, pan-European platform for collecting, analyzing, and sharing threat intelligence, which combines datasets built up in different parts of the project.

What is threat intelligence?

Threat intelligence can be defined as the process of acquiring knowledge from multiple sources about threats to an organisation. Threat intelligence supports informed decision-making on cybersecurity by providing information about threat actors, their techniques, indicators of compromises, and vulnerabilities. The process is essentially collaborative and based on shared datasets.

CONCORDIA's approach

The two cross-sector pilots in CONCORDIA ("Building a Threat Intelligence for Europe" and "Piloting a DDoS Clearing House for Europe") are developing the basic building blocks for a pan-European and cross-sector threat intelligence platform, which conceptually forms a central point of contact for all services within the CONCORDIA ecosystem that are related to threat intelligence.

We are developing the CONCORDIA threat intelligence platform based on three primary principles:

- **Multi-source:** the platform uses multiple datasets available through heterogeneous technologies and providing different data management services (e.g., two clearing houses and their specific services).
- **Combine datasets:** the platform uses algorithms to integrate datasets into new derived datasets (e.g., coupling reported botnet infections and DDoS attacks, see the scenario below).

The screenshot shows the 'No More DDoS' website with a blog post titled 'Setting up a national DDoS clearing house' dated 12 March 2020. The post includes a diagram of the clearing house architecture and a list of participating organizations: SIDN, SURF, CWI, and the University of Twente. The diagram shows a central 'DDoS Clearing House' connected to various 'Service Providers' and 'ISPs'. The list of organizations includes SIDN, SURF, CWI, and the University of Twente.



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](https://twitter.com/hesselma)
+31 6 25 07 87 33