



DDoS Clearing House for Europe (Task 3.2) Cross-sector Pilot Demo

Cristian Hesselman
(SIDN Labs)



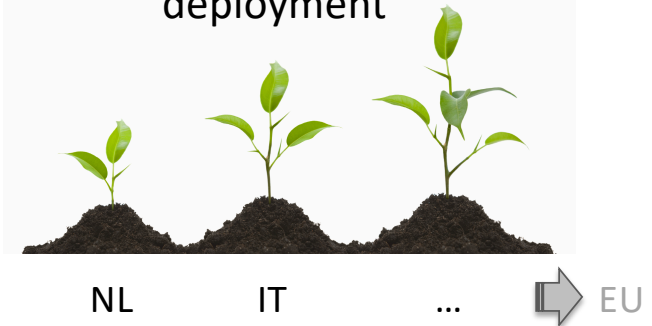


T3.2 objective

- 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**



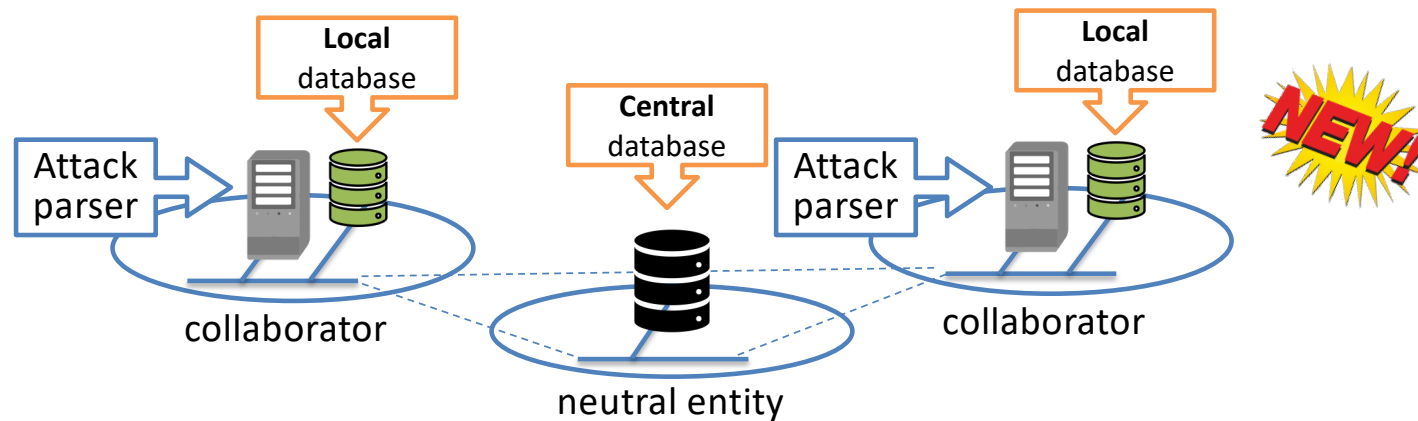
Key challenge: increase to
TRL 5-7 and grow
deployment





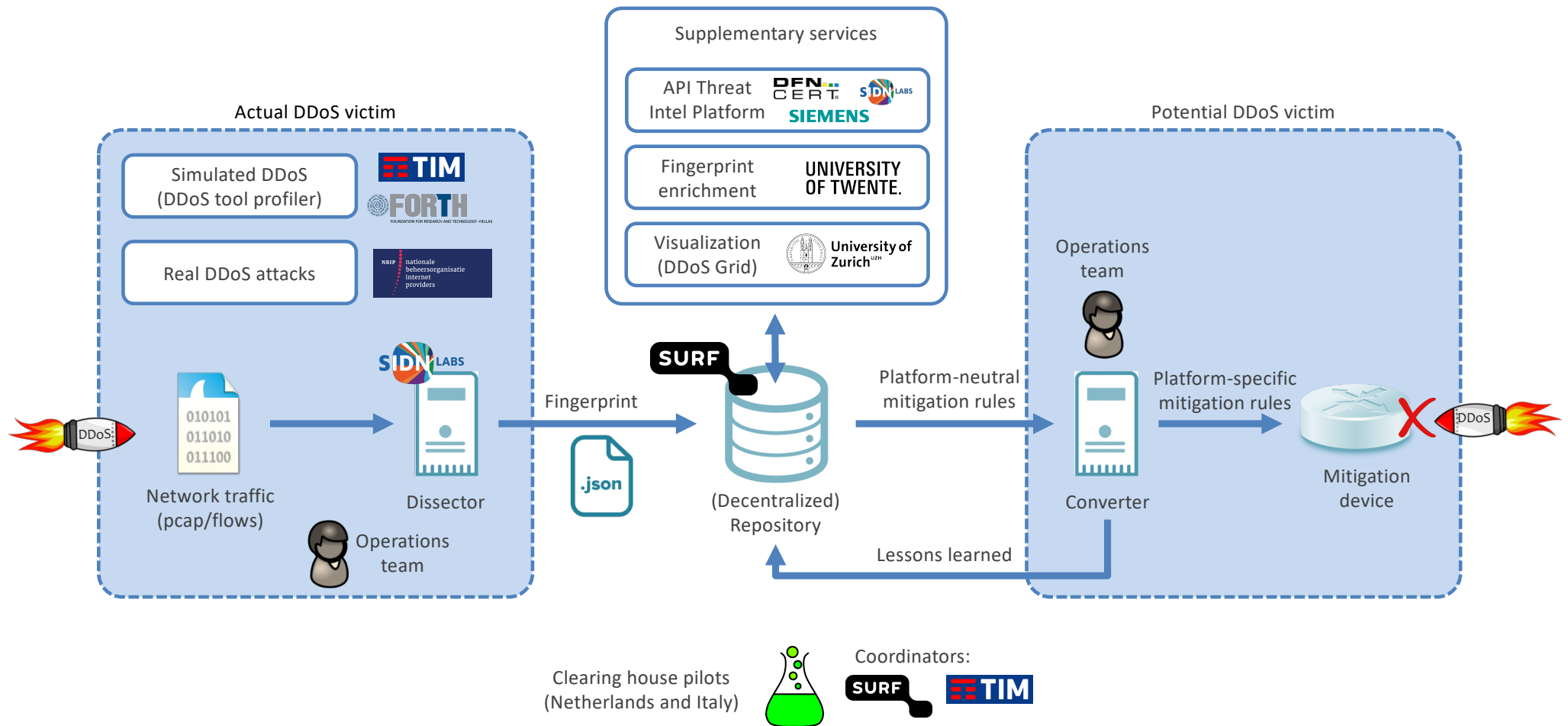
DDoS Clearing House Concept

- 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



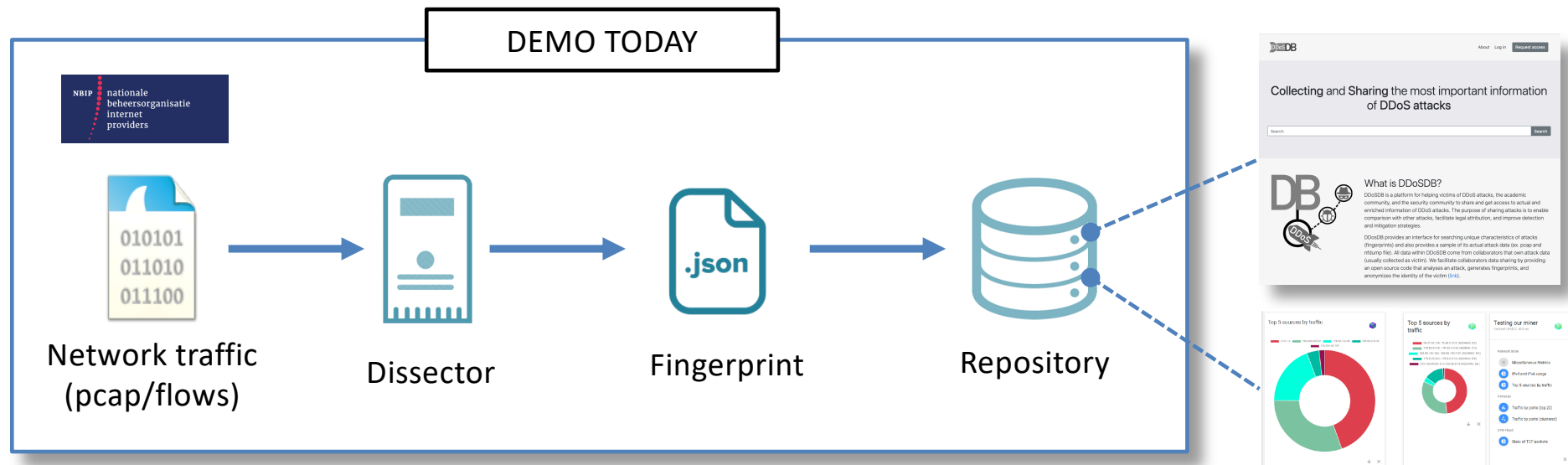


Main Components and Data Flow





Today's Demo



1. Full cycle process (generation, upload, storage)
2. Dashboard for fingerprint visualization
3. Fingerprint enrichment



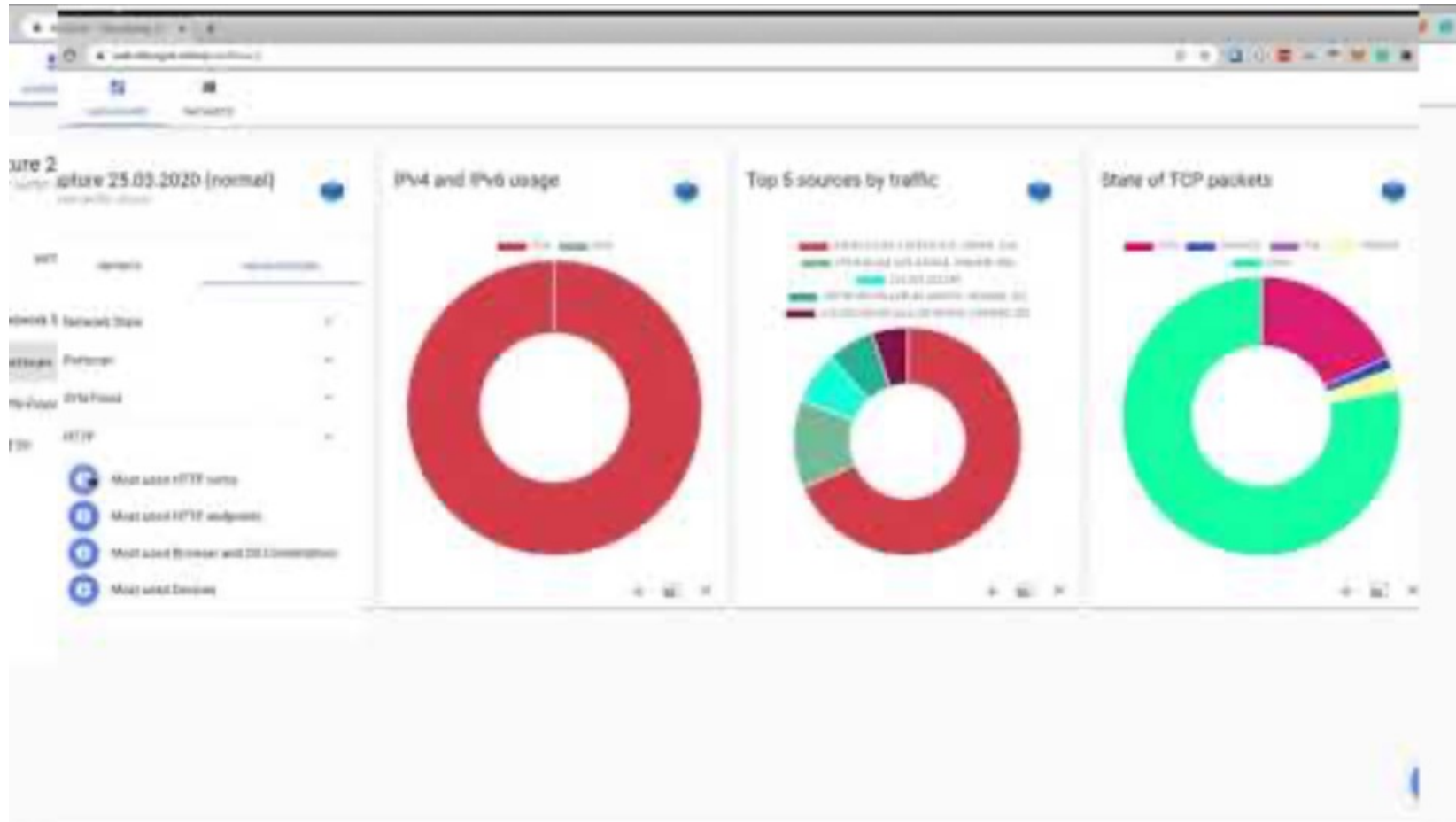
Fingerprint generation, storage, enrichment



<https://www.youtube.com/watch?feature=oembed&v=1QIC3SwwYAU>



Fingerprint visualization (not integrated yet)

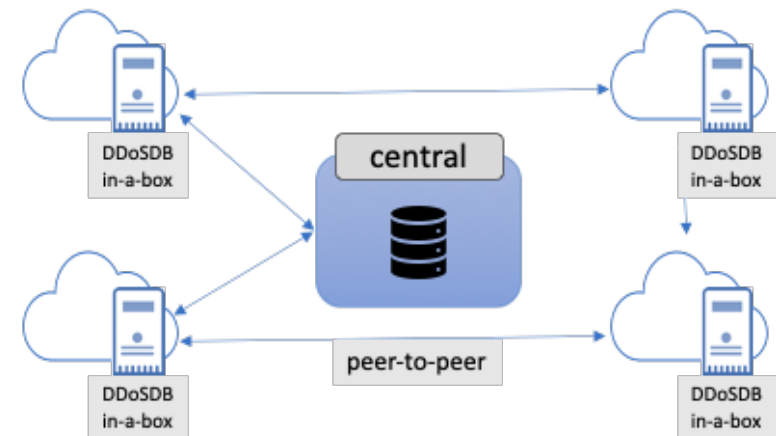


<https://www.youtube.com/watch?feature=oembed&v=5OiCStFuerg>



Next steps

- Aim to deploy system at other partners
 - Dutch pilot and CONCORDIA partners
 - Exchange fingerprints on a regular basis
- Improve software components
 - Dissector: improve DDoS fingerprints
 - Supplementary services on top of DDoS-DB
- Continue demo-driven approach





Further reading

CONCORDIA
Cyber security cOMpeteNCe fOR Research and InnovAtion

Home Consortium Downloads Workshops Events Publicity News Blog Assets

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 more high-level background information, while numbers between straight brackets (I) link to in-depth technical material such as academic papers.

DDoS attack landscape

A Distributed Denial-of-Service (DDoS) attack overwhelms a network with traffic, thus denying servers connected to the network the ability to service legitimate requests from their clients. The attacker typically accomplishes this by simultaneously transmitting traffic from a large number of machines distributed across the internet to the target, for example by infecting those machines with malware that carries out the attack. Another type of DDoS attack is when the attacking machines exhausts a server's resources (rather than swamping the network) [DDoS13]. For example, the attacker could repeatedly start a login session with the server, thus forcing it to make many demanding computations

TWITTER FEEDS

concordia-h2020.eu
follow

concordia-h2020.eu now
Cybersecurity education is important across different areas. Therefore, the courses in the CONCORDIA map are also divided by sectors, so that you can find the most relevant information for your area of business. <https://lnkd.in/dGBhqj3>
#CONCORDIAEDUCATES

concordia-h2020.eu 20h
Searching for a course in #cybersecurity? Courses offered by CONCORDIA partners are displayed on a dynamic map. You can find a course that suits your needs for reskilling, upskilling, or simply learn about this challenging domain. Check out the video [📺](#)
#CONCORDIAEDUCATES

concordia-h2020.eu 15 Sep

SDN LABS
all domains: Cylonspring Vrijlief Internet Keno SIDN Labs Over SIDN

New version of the DDoS Clearing House core components
The next round of improvements to get it deployed

Established up, downloading 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 next step 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 [Cactus](#). 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.

attack mitigation

Gerelateerde items

Ministerie van OCW
→ [Nieuwste anti-DDoS coalitie](#)
Sectoren werken samen tegen DDoS

No More DDoS
Anti-DDoS-Coalitie

Blog

Dutch Anti-DDoS Coalition: lessons learned and the way forward
20 March 2020
Increasing the Netherlands' DDoS resilience together, part I of III
Cristian Heeselman (SIDN) and University of Twente, Remco Poortinga-van Wijnen (SURF), Gerald Schaapman (NBBP) and

Setting up a national DDoS clearing house
12 March 2020
Increasing the Netherlands' DDoS resilience together, part II of III
Cristian Heeselman (SIDN) and University of Twente, Remco Poortinga-van Wijnen (SURF), Gerald Schaapman (NBBP) and

Increasing the Netherlands' DDoS resilience together
9 March 2020
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.



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