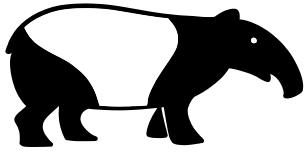
DNS Threat and Privacy Internet Research

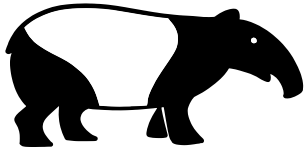
Introducing the DNS TAPIR project



www.dnstapir.se

The Problem

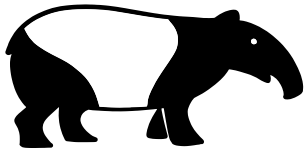
- **Privacy leaks** – By querying DNS, you create data about what you do, which servers you communicate with and much more. This data is often used without respect to the user's privacy.
    - Unique DNS queries are used as a "replacement" for HTTP Cookies, circumventing cookie regulations.
- **Cyber Security** – Malicious software use DNS for communication and pinging home. These cyber operations needs to be monitored and a response needs to be formed.



What can be done?

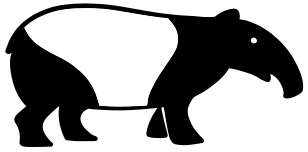
- The server that handles queries and responses, the DNS resolver, produce logs that include privacy data
- This data can be aggregated, gathered and analysed in almost real time
- One result of the analysis is threat warnings, that may change filters and help protect users and networks

Aggregated DNS resolver logs can be analysed and used for cyber security monitoring without privacy issues.

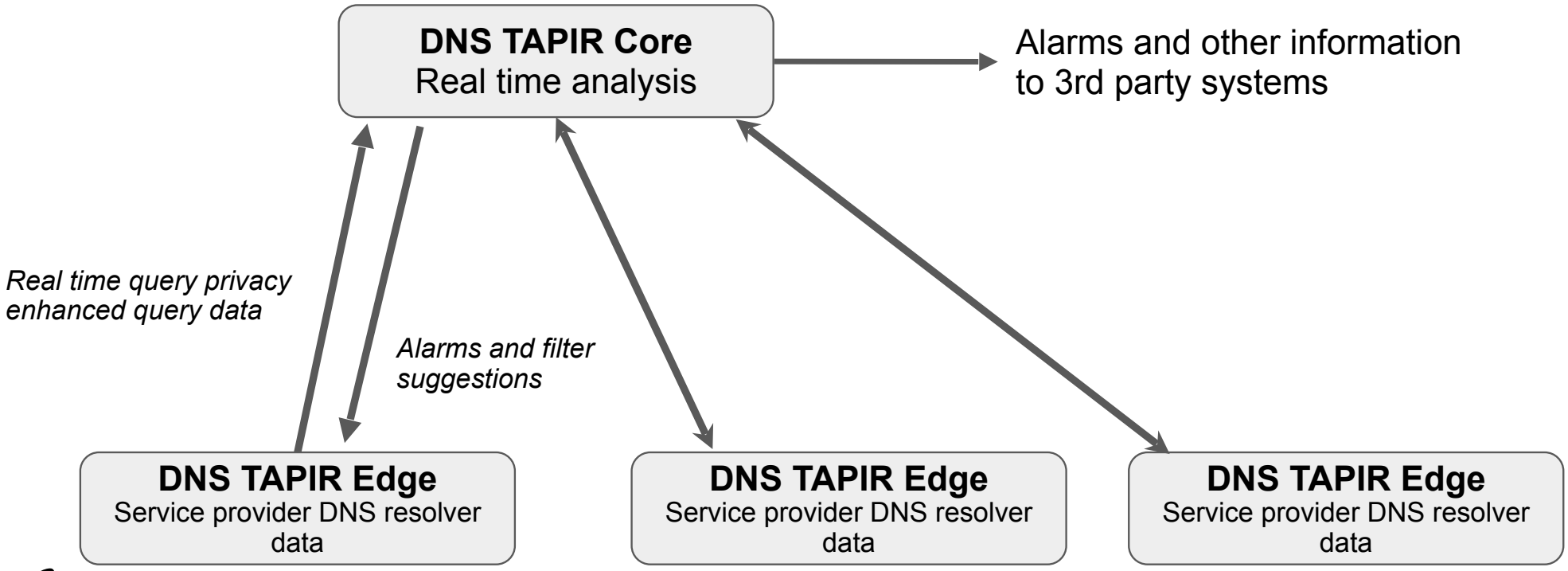


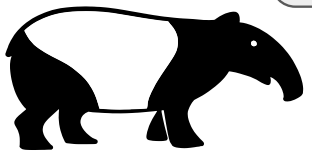
The DNS TAPIR software

- **DNStapir Edge** – A service that runs close to a DNS resolver that aggregates logs and forwards data to the cloud service. Installed in service provider's networks and similar places.
- **DNStapir Core** – The cloud service that aggregates, analyses and annotates data, and produces different alerts. The cloud service can be divided in a federated network of instances without affecting the user's privacy.

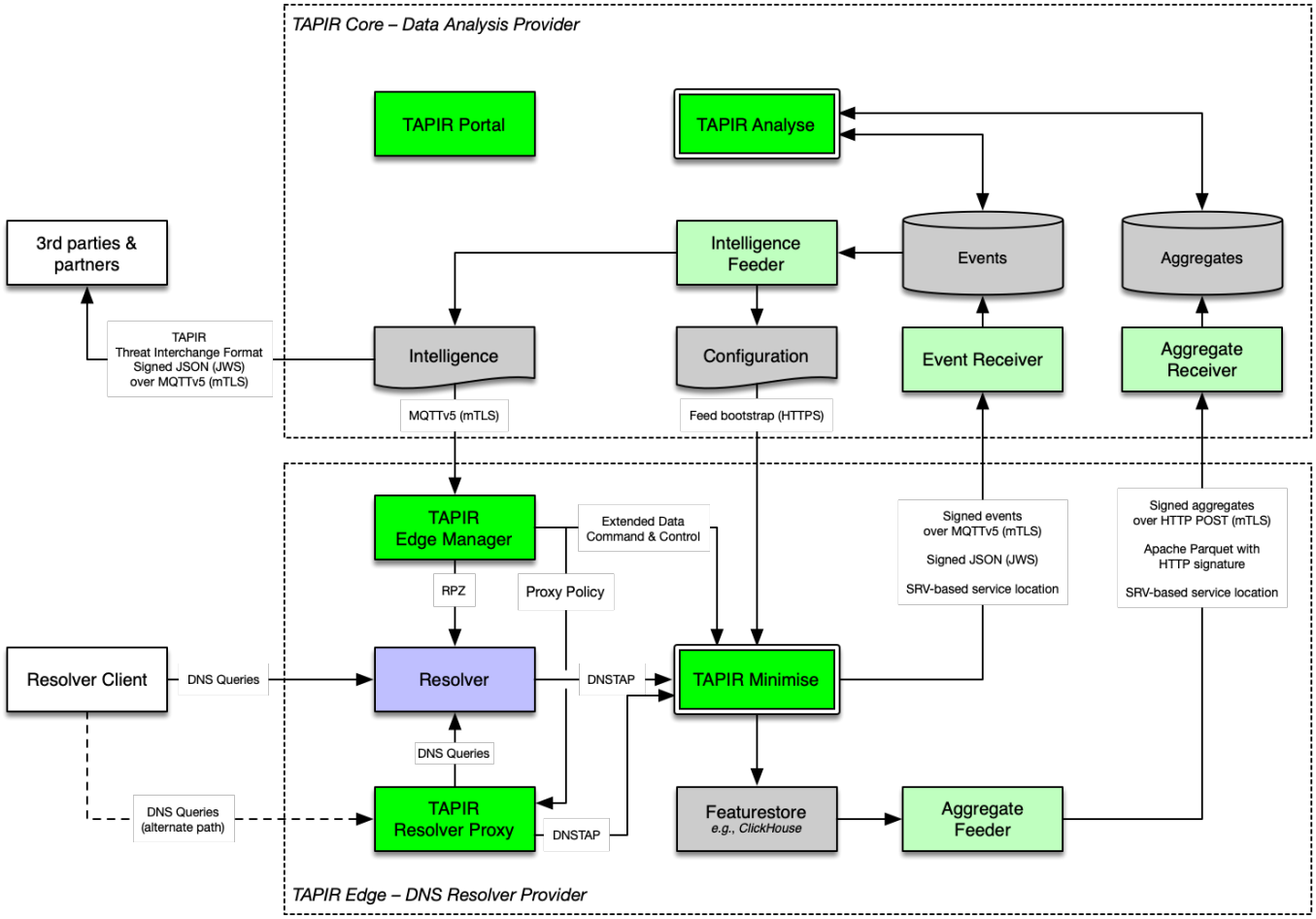


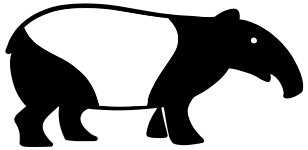
The DNS tapir service overview





Detailed System Overview

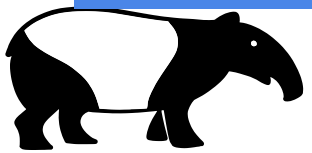




www.dnstapir.se

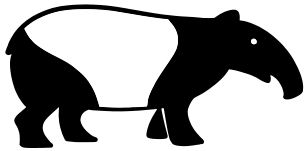
DNS TAPIR Project Phases

Phase 1	Phase 2	Phase 3
• Develop PoC • Establish project • Plan coming phases	• Build production platform • Integrate with partners • Build organisation for maintenance of code and platform	• Normal operations • Algorithm maintenance • Data analyses • Code & container maintenance



Partners in Phase 1
Architecture and Proof of Concept

- Main Funding by PTS, Post & Telestyrelsen, Sweden – the “Robust DNS” project
- Resources provided by Sunet/Vetenskapsrådet, Internetstiftelsen and Netnod
- Partners



www.dnstapir.se

Next steps for DNS TAPIR

- Set up a cloud service for early adopters
- **GET MORE DATA IN OUR FEED!**
- Discuss with service providers, public sector and enterprises on how to cooperate to strengthen the cyber security for everyone
- Find a long-term funding solution for the Open Source project as well as operations of the core