# EuroHPC: Security Overview of the HCSA

Subtitle (if applicable)

**Scott Campbell**
Security Architect

SIG-NOC, Utricht, NL
9-10 April, 2026

# Security Overview

The Security and Trust components of the HCSA are composed on three basic groupings:

- **Technical**: Technical controls for reducing risk as implemented by GÉANT for the HCSA core network
- **Policy**: Organizational controls put in place to address issues around process and risk management as described in ISO 27001
- **Security Incidents**: Process implemented specifically for HCSA security incidents that extend beyond the boundaries of a single participating NREN

*Given time constraints, this is a very short overview of these Very Exciting topics*

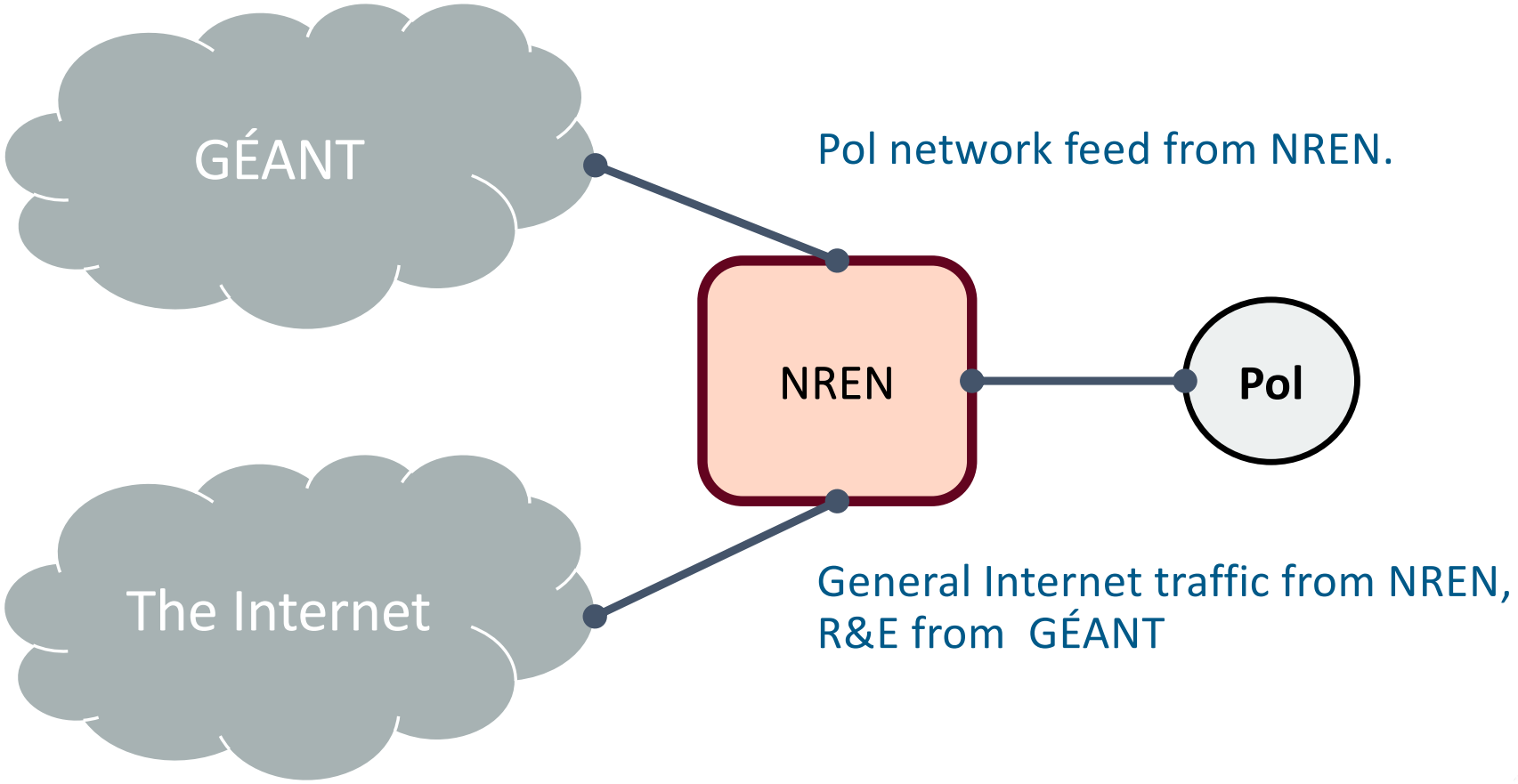
# Technical Controls Overview

Individual technical controls can be broken out into three basic types:

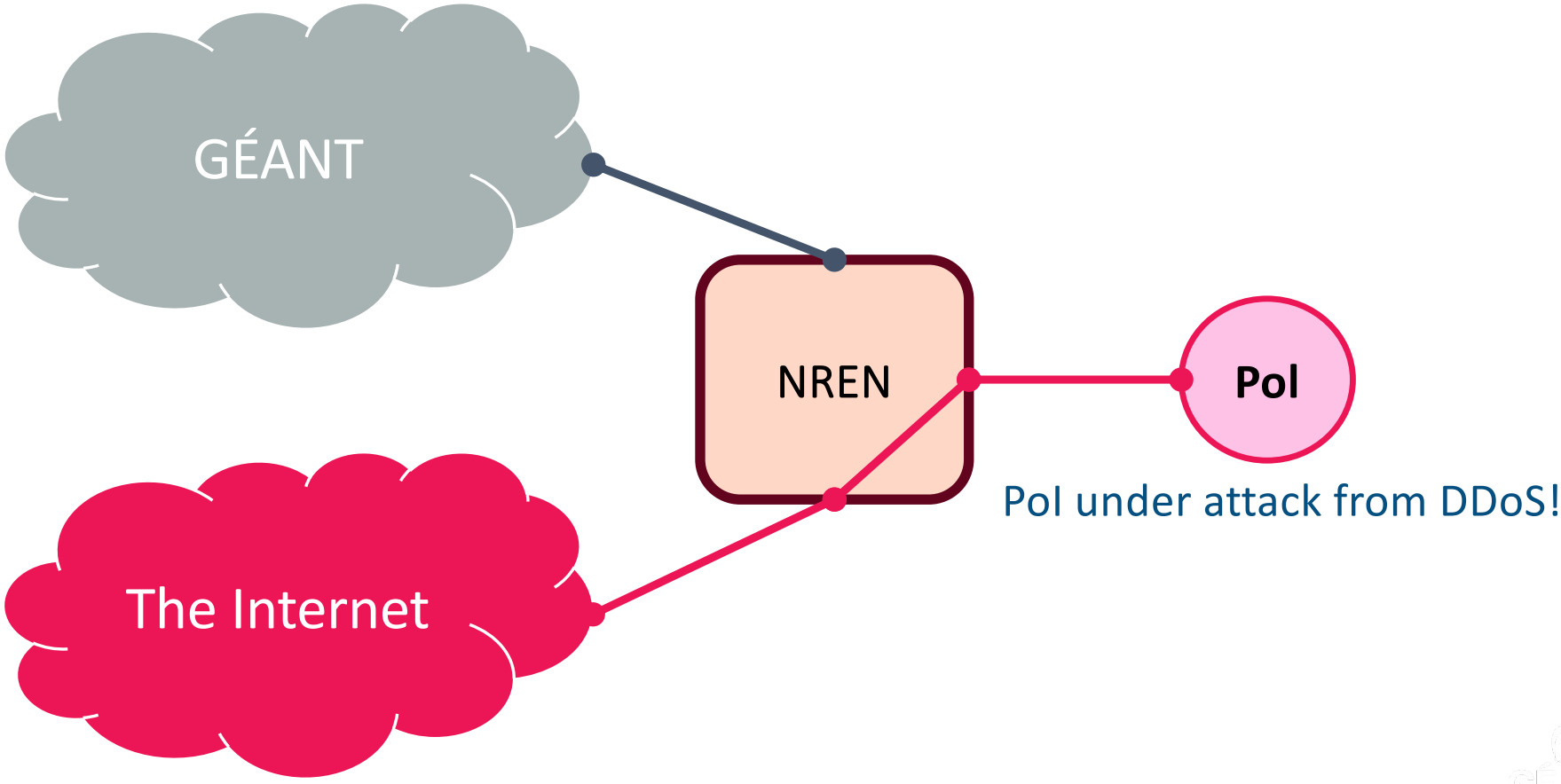
- Routing Security
- Traffic Filtering: specifically designed for hostile traffic
- Traffic Control: General traffic modifiers

But first a quick note on limitations in technical controls

# Technical Controls: Scope of Influence



# Technical Controls: Scope of Influence



# Technical Controls: Scope of Influence

The footprint of the HCSA is complex and has overlapping components with non-HCSA networking.

This means that a PoI connectivity can be influenced by attacks and errors *outside* of the HCSA.

For those here this may be more of an “obvious” thing, but it is worth emphasizing: if a PoI is under attack from a source that GÉANT has no control over, there are no (non-heroic) technical controls that GÉANT has to address the situation.

# Technical Controls: Routing Security

- Follow best practices as defined in MANRS.
- RPKI validation for route updates from downstream and partner networks
- Filtering on accepted prefixes

MANRS : Mutually Agreed Norms for Routing Security (MANRS) is a global initiative that helps reduce the most common routing threats.

RPKI : Resource Public Key Infrastructure (RPKI) allows Local Internet Registries (LIRs) to request a digital certificate listing the Internet number resources they hold. It offers verifiable proof that a holder's resources have been registered by a Regional Internet Registry (RIR).

# Technical Controls: Traffic Filtering

- Spoofing defense ala MANRS
- DDoS detection
- DDoS mitigation (internal tools - flowspec, scrubbing)
- DDoS mitigation (external tools - stateless upstream filtering)

Filtering is designed to specifically address hostile traffic

DDoS specific risk – high return on low cost for the attacker. Useful as a lever for other attacks.

Upstream filtering for commodity transit feeds.

# Technical Controls: Traffic Control

- FlowSpec using Firewall on Demand

Traffic Control addresses more flexible tooling for general traffic manipulation.

# Policy

GÉANT has taken security measures in the organisation and network that are based on risk management as described in ISO 27001. These measures ensure protection against most common attacks according to latest insights and common best practices.

As part of this process, GÉANT has implemented a set of policies and security measures according to the GÉANT Security Baseline, which is based on ISO 27002 and NIST best practices.

# Security Incidents

Most security incident decision making can be mapped to the incident response already defined for purely network related issues.

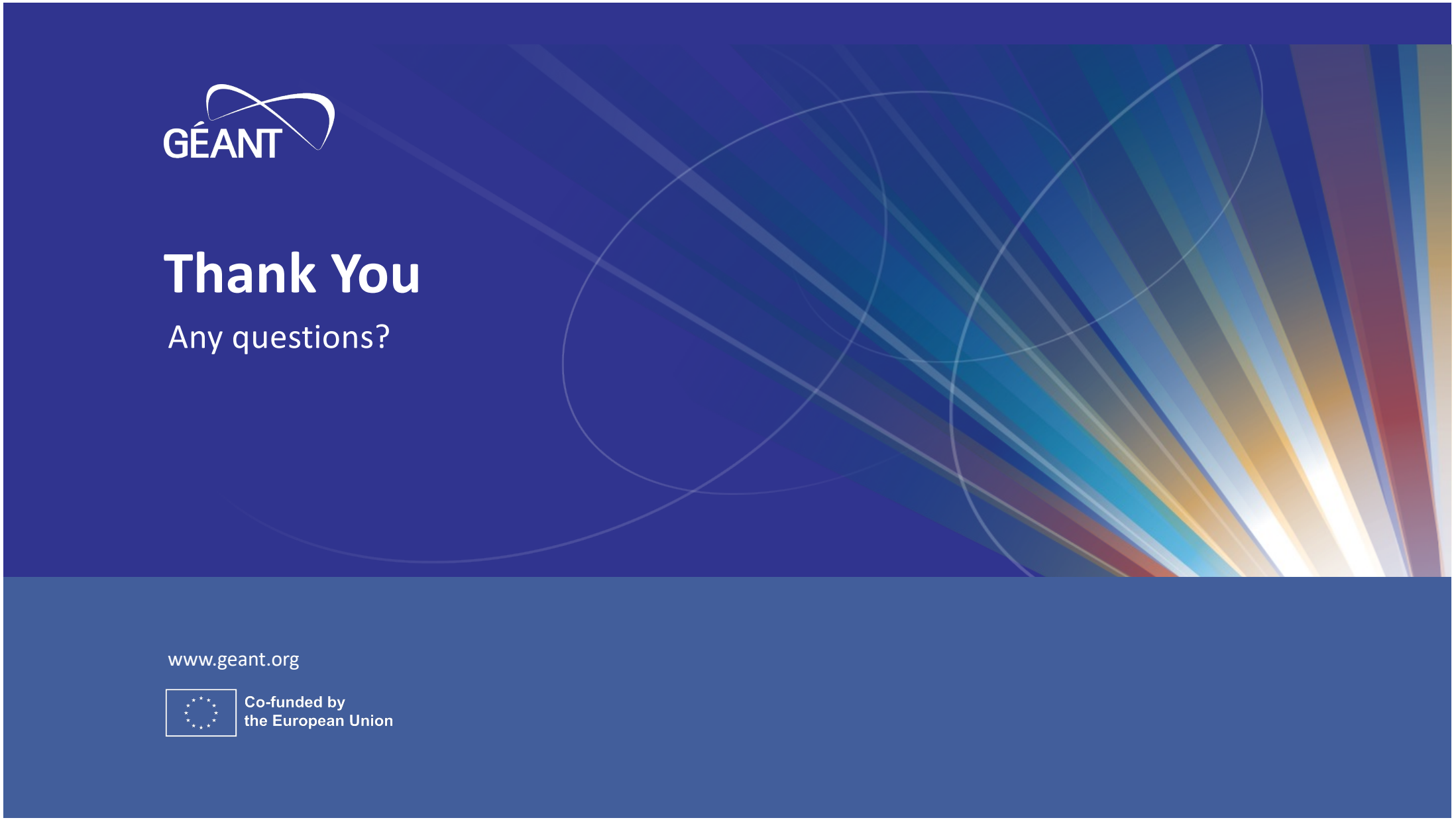
Each NREN and each PoI site will have an identified security incident response point of contact

The point of contact will coordinate the analysis and resolution of security incidents.

When possible, incident response playbooks should be developed for cross-NREN and each PoI site incidents.

These will incorporate input and feedback form the security teams from the NREN and each PoI sites.

There will be one (1) email address for reporting security incidents by project partners and by users of the infrastructure. Tentative address will be hcsa-security@geant.org, with the final choice to be communicated to the PoI sites.


GÉANT
Thank You
Any questions?
www.geant.org
Co-funded by
the European Union