“Fighting NeMo”

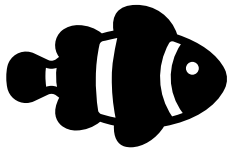
How to tame the beast and make it work for the Géant Network.

Ryan Richford
NETWORK SECURITY ENGINEER

Security Days, Prague.

Who are GÉANT SOC?

- Security Ops (GÉANT Network)
- Daily security and maintaining GÉANT Services
- Just over one year old
- Three people



What is NeMo?

- GÉANT's DDoS Cleansing & Alerting service
- Improved Network visibility & mitigation capability
- Offered to all NREN's as a service & maintained by SOC

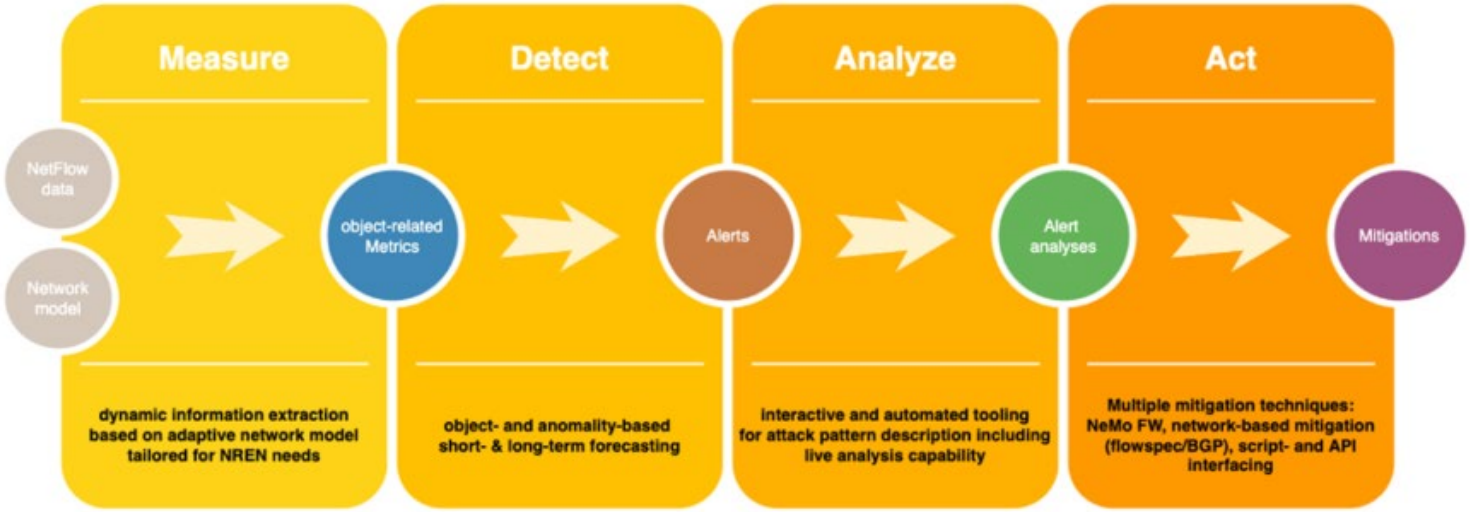
DDoS Cleansing and Alerting

Taking DDoS detection and mitigation to the next level

The increasing volume (frequency, duration and size) of (distributed) denial-of-service ((D)DoS) attacks mean that we need improved detection and response capabilities. As a complement to firewall-on-demand, DDoS Cleansing and Alerting (DDoS C&A) utilises NeMo to alert on potential (D)DoS attacks and a variety of mitigation mechanisms to thwart the impact of these attacks.

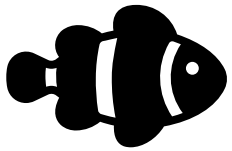
The GÉANT DDoS C&A Service aims to:

- Protect the GÉANT core network and related infrastructure from (D)DoS attacks.
- Protect (for subscribed customers) NREN uplinks to the GÉANT network from being filled as a result of (D)DoS attacks targeted at the NREN and/or NREN institutions.



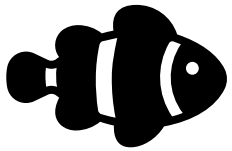
NeMo's History?

- 12+ years of experience by DFN-CERT in DFN network
- Continued development in GN4-3 & GN5-1, WP8
- Detection component utilising flow data + network model
- Mitigation components (current/future*):
  - Integration with Firewall-on-Demand / BGP FlowSpec*
  - NeMo Mitigation (cleansing engine)
  - API-integrations possible
- Open Source (licensed for NREN use)



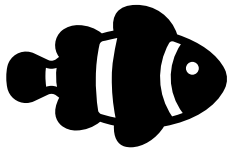
Differences in the GÉANT & DFN use case

- DFN & GÉANT as institutes/company
- DFN Focuses on end users and Universities
- GÉANT Focuses on NREN uplinks and providers



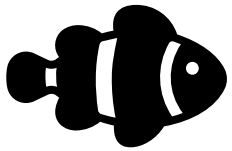
Creating a full/functional service

- Users must be able to access their own accounts for analysis
- NREN’s must be able to see their objects (Ases) ONLY
- NREN’s must understand the process for mitigation
- NREN’s must be able to provide feedback



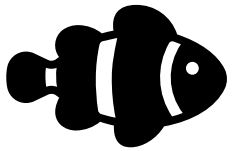
GÉANT SOC's operational requirements

- Processes & Document's (user guides for SOC & NREN's)
- Communication channels for NREN's
- Troubleshooting & Maintenance
- Training of other Internal teams & NREN's



Refining the DDoS C&A service

- NREN size differences meant trigger sensitivity categories were necessary
  - Default
  - High
  - Low
- Reporting (email analysis) was created & can be opted into by NREN's

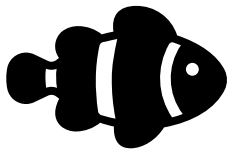


Future of the DDoS C&A service

- Integration with FOD
- NeMo's 'own' mitigation (moving away from A10)
- Steady feature additions from DFN

Own Info / deployment:

- GÉANT NeMo deployment:
  - soc@geant.org
- Own deployment / other Qs:
  - nemo@lists.geant.org



Thank You

Any questions?

www.geant.org

Co-funded by
the European Union