



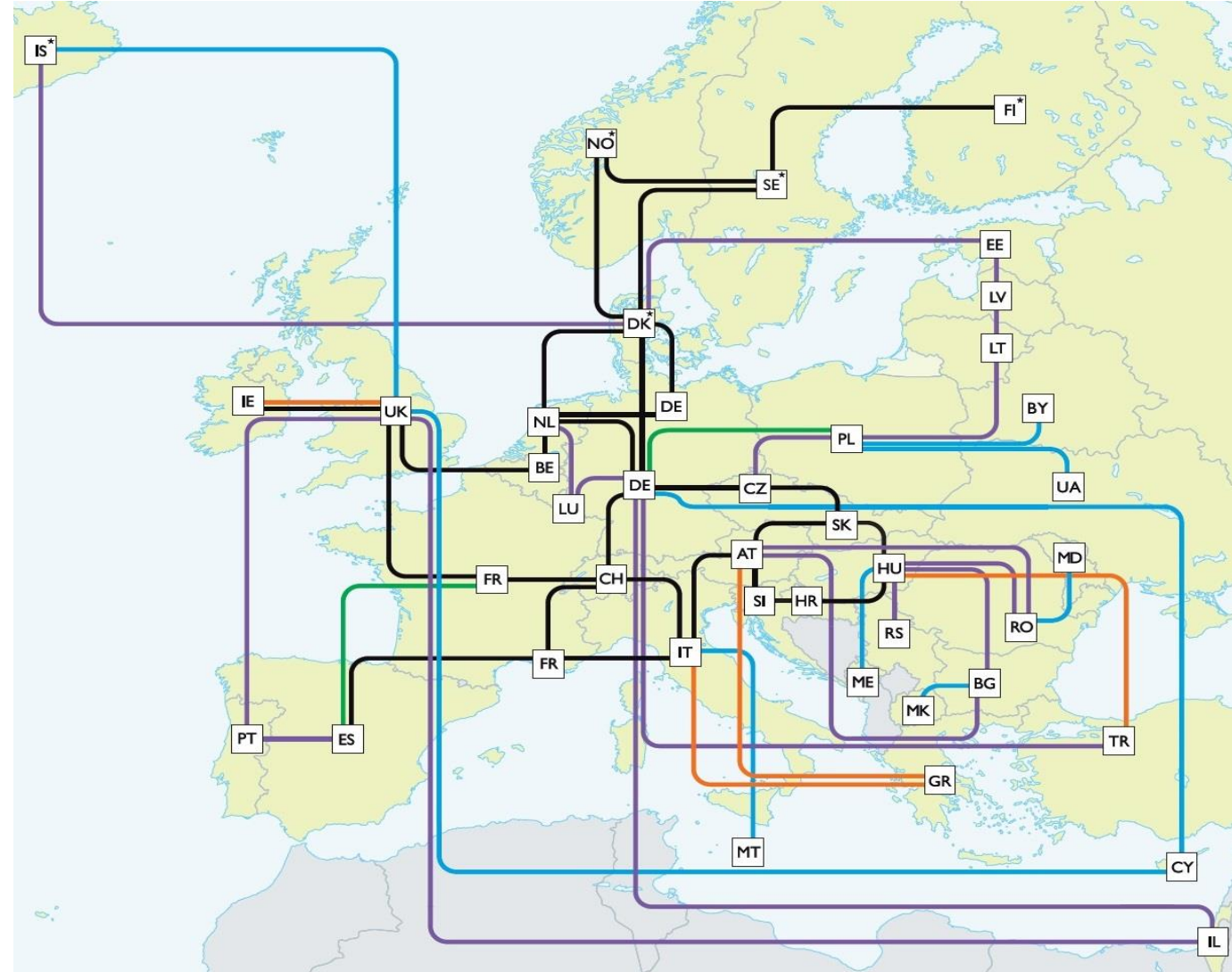
# NREN & ISP Security Working Group 2014 Review

Wayne Routly, DANTE

44<sup>th</sup> TF-CSIRT Meeting  
19 September 2014  
Rome

# GÉANT : Who What How

- State of the Art Pan-European Network
  - .....Transit Network....ISP
  - 31 Collection Devices (Juniper MX)
  - 50 Million End Users (65 Countries)
- Tb/s Network
  - 100s PB of Data
  - 15+Millions IPs
  - 1000 Devices
  - Unusual Traffic – Quasi R&E DoS
- Truly Global
  - Interconnects (I2, TEIN, Ubutunet)
  - NRENs - 43
  - Commercial & Commodity Traffic



- **Objectives:**
  - Background to Working Group
- **Achievements: Today (2014)**
  - NSHaRP security toolset upgrade
  - Response to 2013 Audit
- **Challenges: Tomorrow (GEANT4)**
  - Outcomes from 2014 Audit
  - New Systems, New Challenges



**Demonstrate Leadership**

# Security Working Group Objectives

**High Level  
Management  
Review**



**Share  
Knowledge of  
Current  
Threats**



**List  
Recommended  
Physical  
Security  
Approaches**



# Working Group Members



**Wilfried Wöber**

[wilfried.woeber@univie.ac.at](mailto:wilfried.woeber@univie.ac.at)



**Serge Droz**

[serge.droz@switch.ch](mailto:serge.droz@switch.ch)



**Doug Pearson**

[dodpears@ren-isac.net](mailto:dodpears@ren-isac.net)



**Wayne Routly**

[wayne.routly@dante.net](mailto:wayne.routly@dante.net)



**Lionel Ferette**

[lionel.ferette@enisa.europa.eu](mailto:lionel.ferette@enisa.europa.eu)



**Dave Monnier**

[dmonnier@cymru.com](mailto:dmonnier@cymru.com)



**Jacques Schuurman**

[jacques.schuurman@xs4all.net](mailto:jacques.schuurman@xs4all.net)



**Andrew Cormack**

[Andrew.Cormack@ja.net](mailto:Andrew.Cormack@ja.net)

## Achievements: Today (2014)

# Achievements: Today (2014)

- NSHaRP Infrastructure
- Nessus
- Web Camera's in PoPs
- Firewall on Demand
- Dedicated Security Officer





# NSHaRP Changes

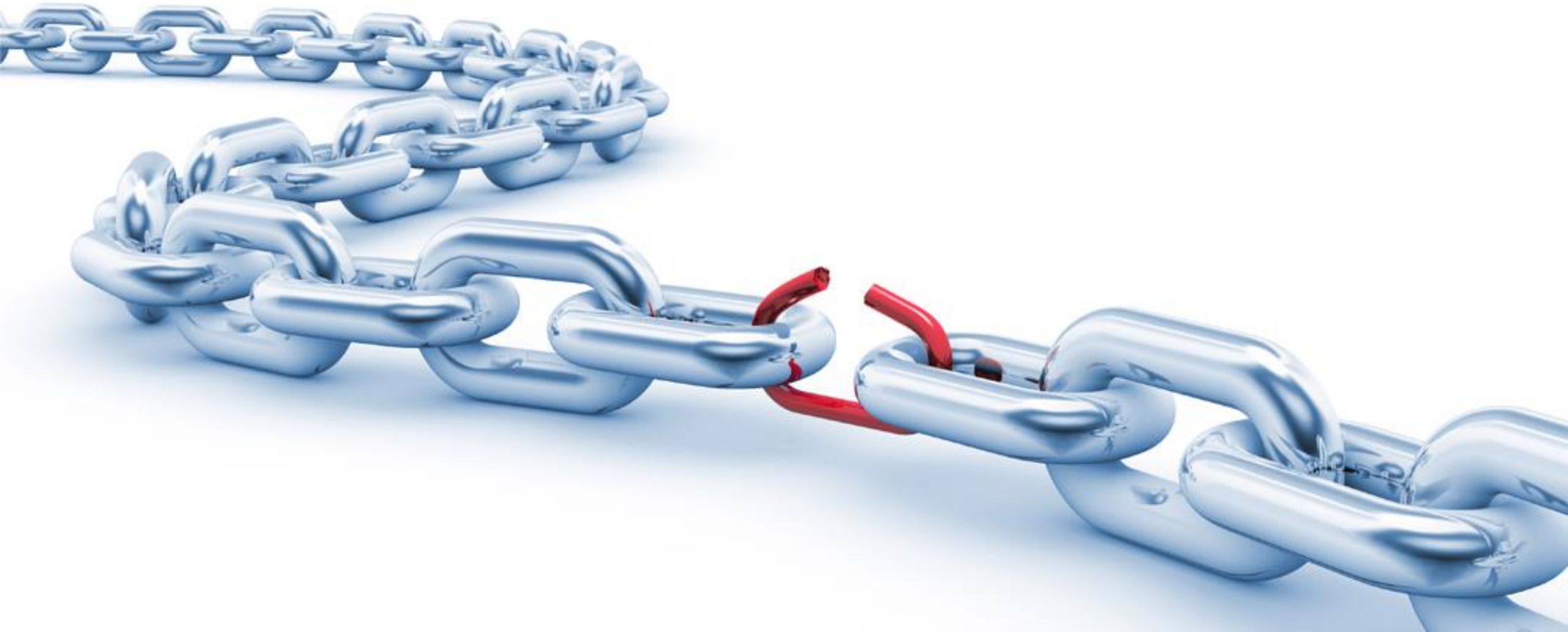
- Sampling Rate 1/100
- v5 – v9
- Redundant Fan-out Servers
- Increased Net Flow Demand



<<< New Trouble Ticketing System; New Anomaly Detection Tools; New Anomaly Type Pallet >>>

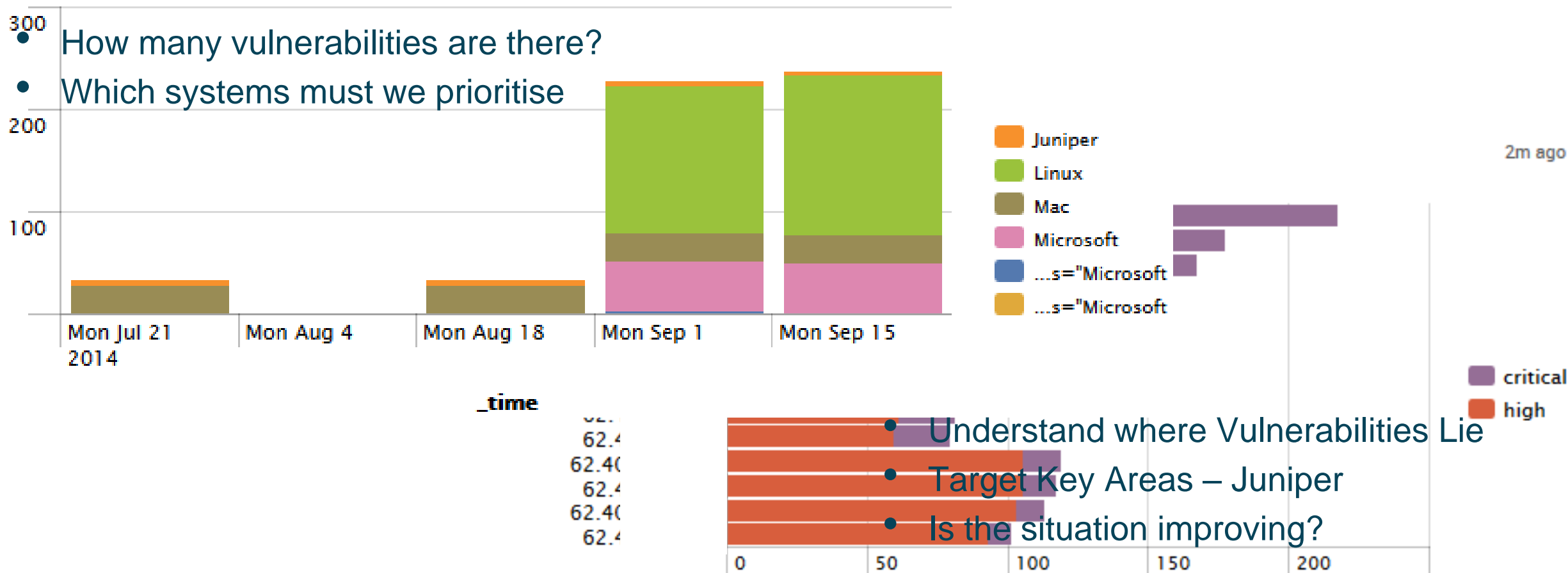


# Vulnerability Assessment – Finding that Weakest Link



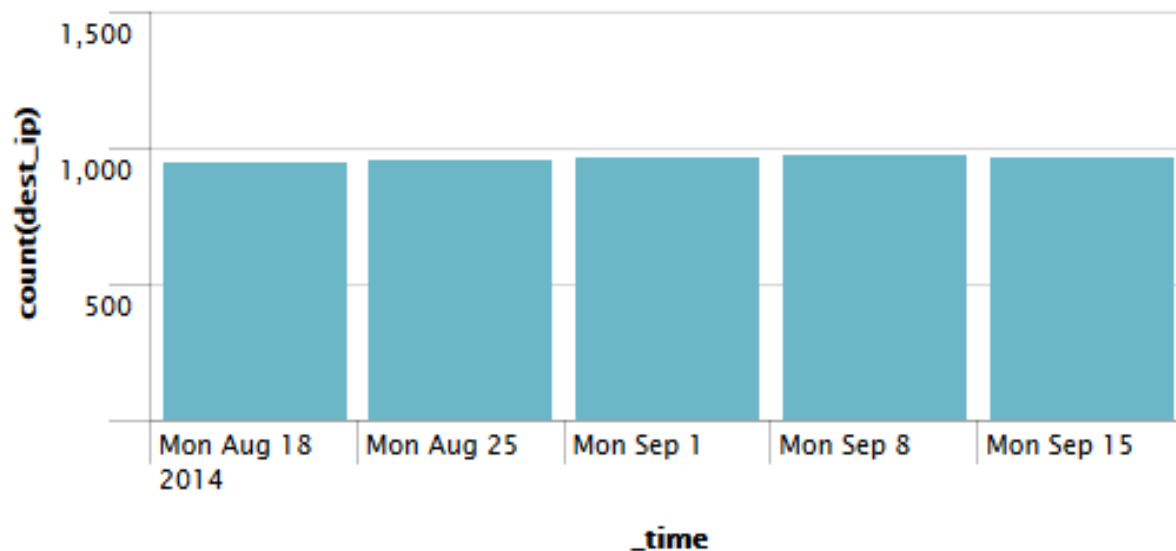
# Understanding Your Network.... Nessus

## Number of vulnerable systems by OS



# Controlling Your Network.... Nessus

Alive hosts (weekly basis) found on 3 GEANT zones



- When last did we see this host?
- Has it had a vulnerability scan?

- Which zones are vulnerable?
- External Zones must be prioritised

New alive/dead hosts (previous and this week)

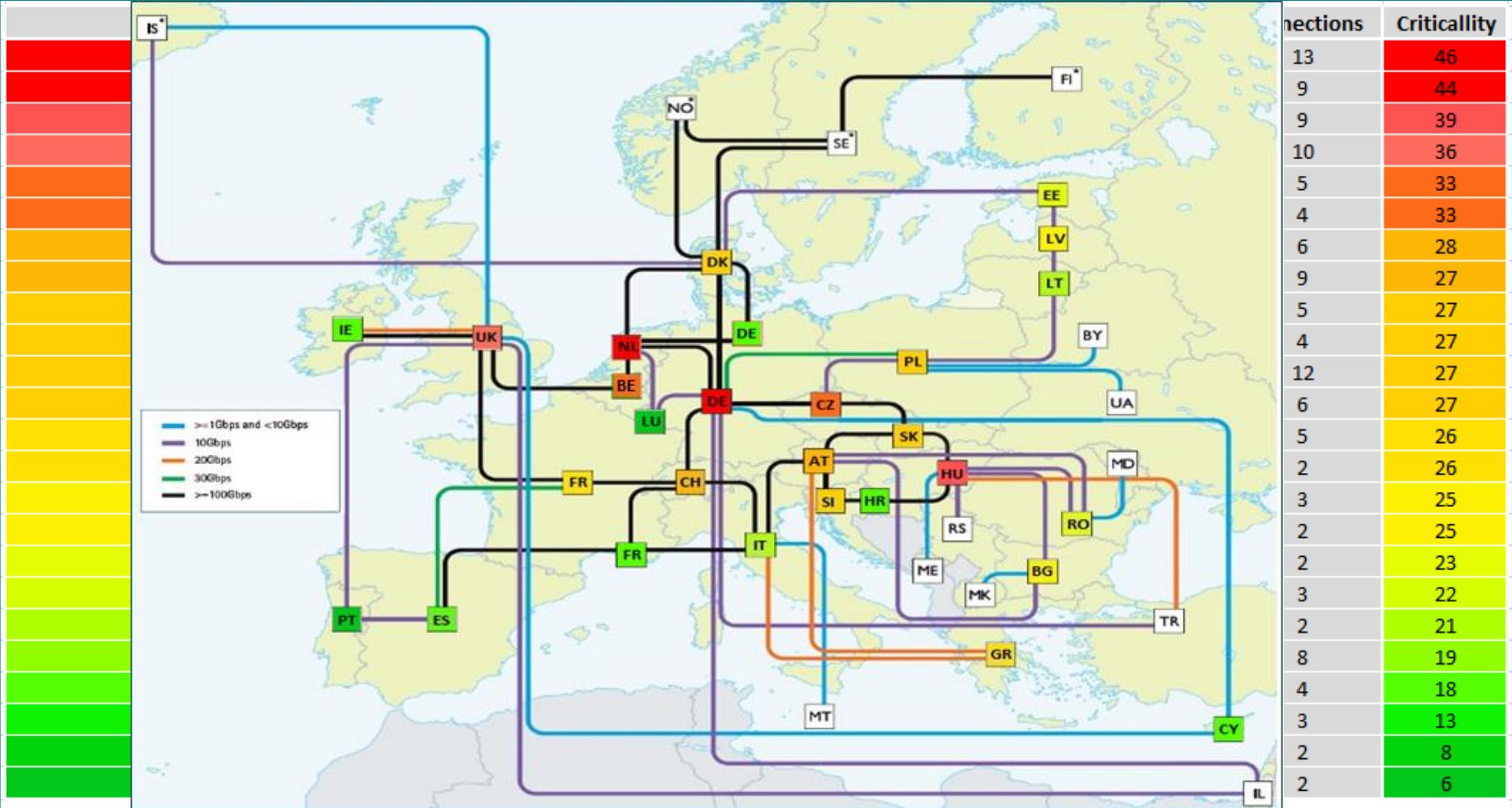
5m ago

dest_ip ↕	count(dest_ip) ▲
62	1
62	1
62	1
62	1
62	1
62	1
62	1
62	1
62	1
62	1

« prev 1 2 3 next »



# Web Camera's In PoPs – Prioritise Locations



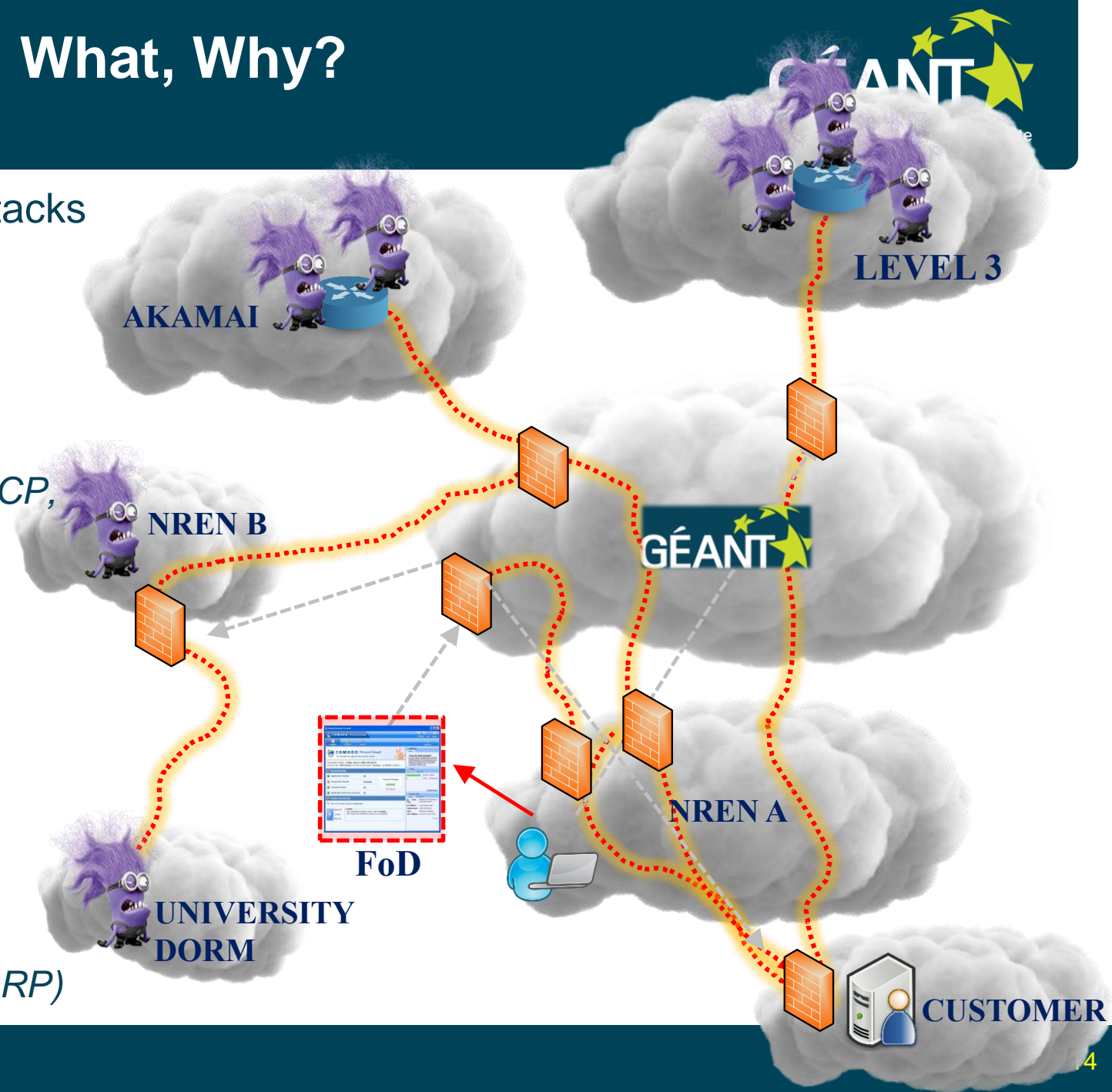
\* Criticality is greatly increased for that PoP based on its location



# Firewall on Demand – Who, What, Why?

..... **better tools** to mitigate **transitory** attacks and anomalies

- “**Better**” in terms of
  - **Granularity:** Per-flow level
    - *SRC/DST IP/Ports, protocol type, DSCP, TCP flag.....*
  - **Action:**
    - *Drop, rate-limit, redirect*
  - **Speed:** More responsive
    - *(Seconds / Minutes vs. Hours / Days)*
  - **Efficiency:**
    - *Closer to the source, Multi Domain*
  - **Automation:**
    - *Integration with other systems (NSHaRP)*





# Firewall on Demand – Intuitive Interface

Firewall Rules

20 records per page

ACTIVE

PENDING

ERROR

DEACTIVATED

Search:

Showing 1 to 1 of 1 entries

Previous

1

Next

Name	Match	Then	Status	Applier	Expires	Response	Actions
<a href="#">firstrule_GEANT_I6W1NM</a>	<div>Dst Addr</div> <div>Src Addr</div> <div>Protocols</div> <div>SrcPorts</div>	<div>rate-limit</div> <div>100k</div>	ACTIVE		2014-09-18	Successfully committed	<div>Edit</div> <div>Deactivate</div>

Showing 1 to 1 of 1 entries

Previous

1

Next

- Integrated into NSHaRP
- Dynamic Auto Creation & Expiration
- Federated Logon





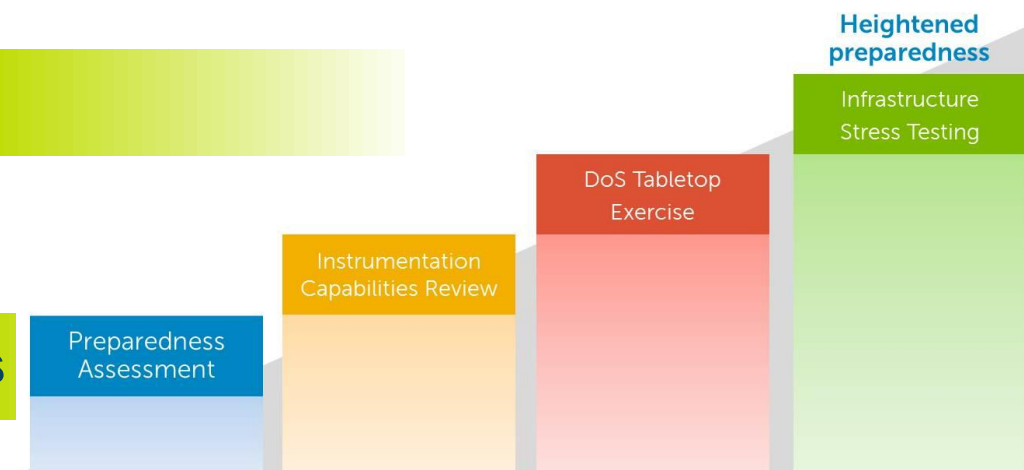
## Challenges: Tomorrow (GEANT4)

**Walled Gardens: Vulnerable Systems Management**

**Net Flow Data Anonymisation**

**Ownership of Virtual Machines (Life Cycle)**

**Stress Testing - Targeted Ingress and Egress Scans**



# Security WG Report

## *Process & Technology Findings*

**Implement IDS: Verify all certificates in the organisation**



**DANTE & TERENA – “Sanity Checks”**

**Appetite for # Vulnerabilities: CVSS Length of exploitability**



**We must inspire a  
commitment to security  
rather than merely  
describing it**

– Mich Kabay





**Thank you**

**Any questions...even the funny ones?**