



GÉANT

ASSOCIATION

Networking • Services • People

Drowning in Logs

Evangelos Spatharas

TF-CSIRT Meeting

Tallinn 24 September 2015

- What logs are and why are so important
- GEANT logs everywhere
 - How do we monitor our logs
 - Dashboard panel logs
 - Do we have complete visibility?
- Plan to accommodate missing logs
 - Problems with per volume licensed tools
- Open source logging tools
 - Selected tools for evaluation
- Q & A
- FoD update

What logs are and why are so important?

Special files



Detective Technical Control



What logs are and why are so important?

Evidence



What logs are and why are so important?

.. Uncover configuration mistakes



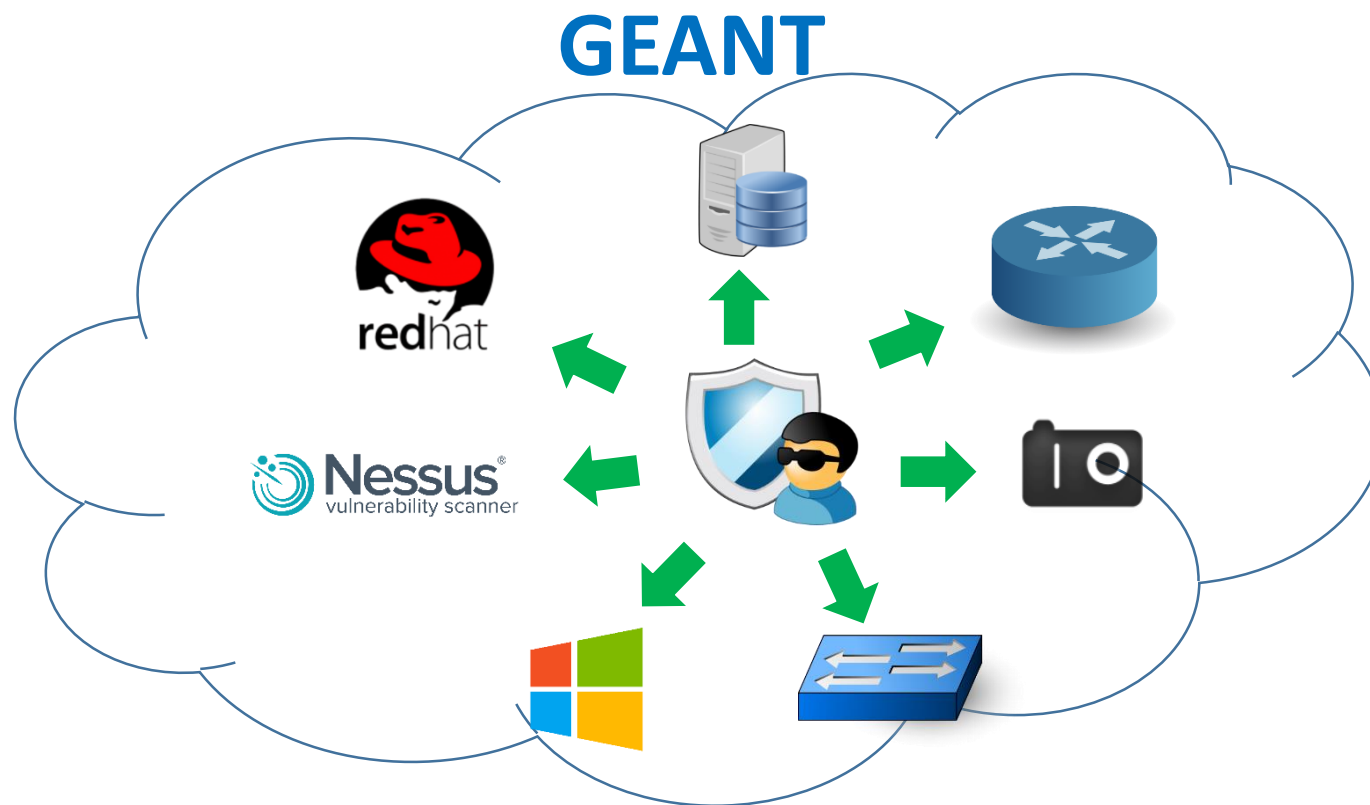
GÉANT system logs everywhere

Multiple sources

- > 150 Win VMs
- + > 200 RHEL VMs
- + > 40 Hyper-Vs
- + > 30 IP cameras
- + 31 Juniper MXs
- + Many PoP switches

=~

8-9M

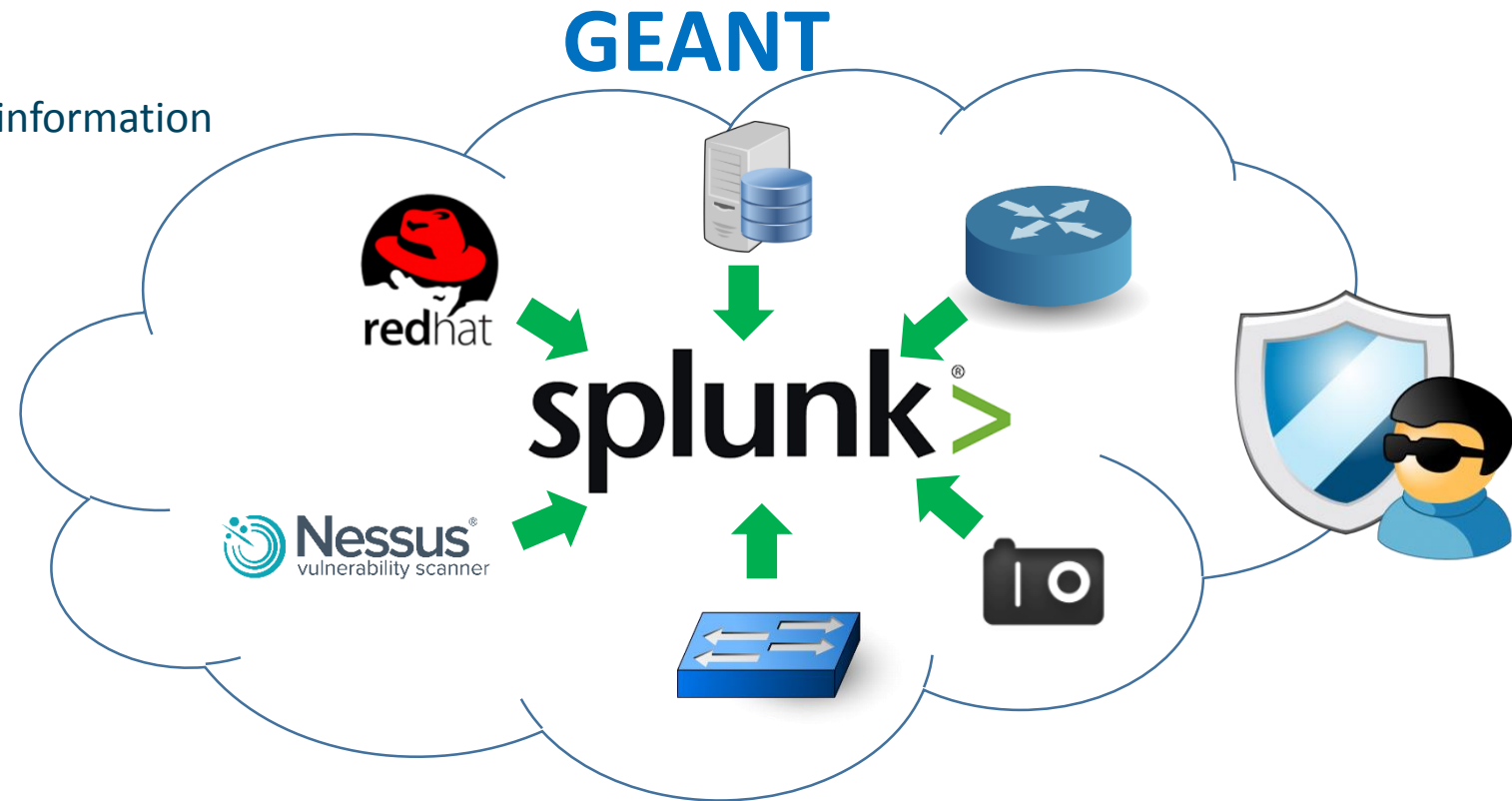


HELP!

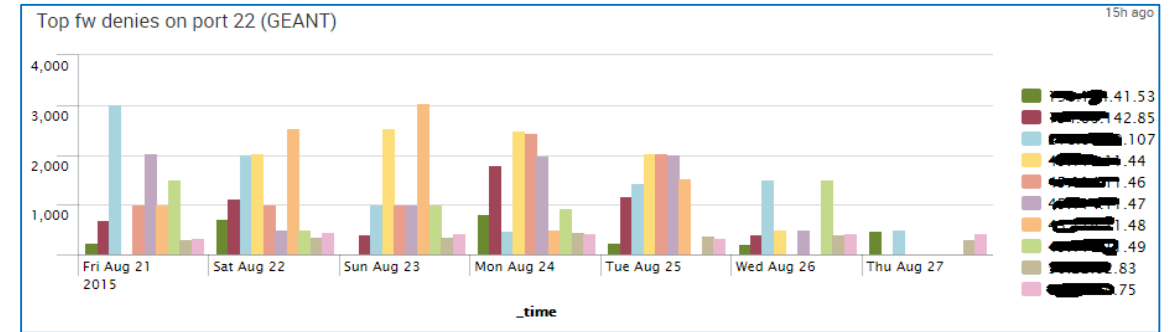
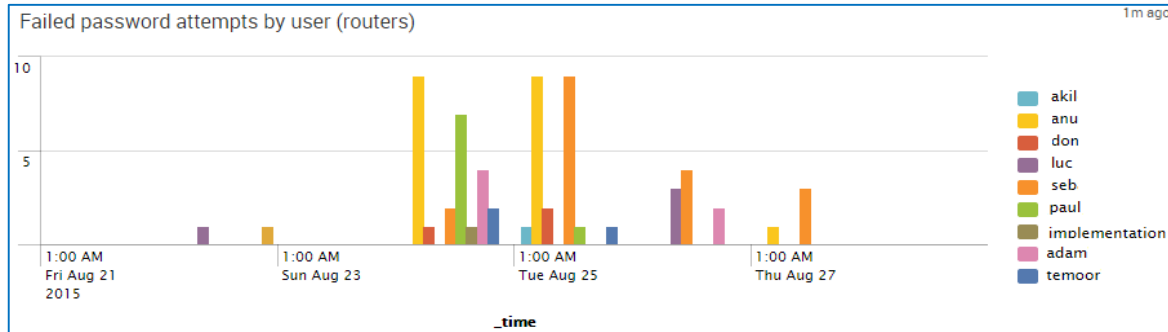


How do we monitor our resources?

- Single interface for all of types of information
- Data correlation
- Powerful search and analytics
- Alerts
- Bigger picture
- Operations and Security solution



Routers/Switches dashboard

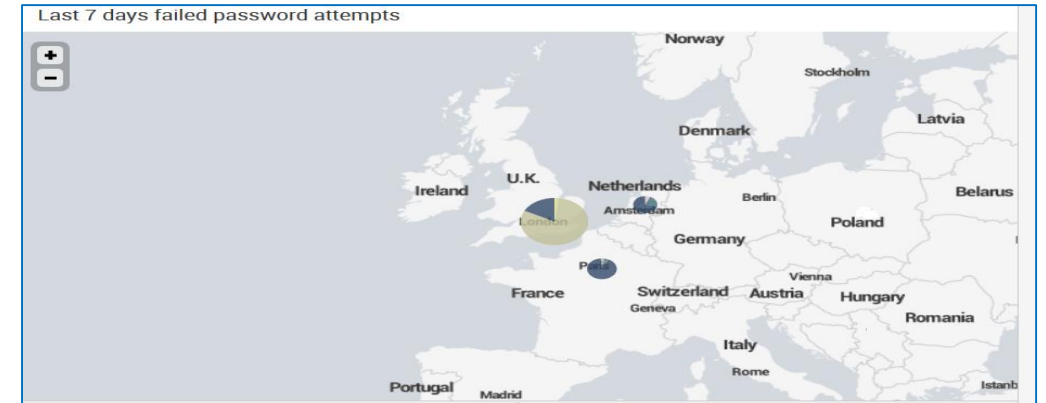
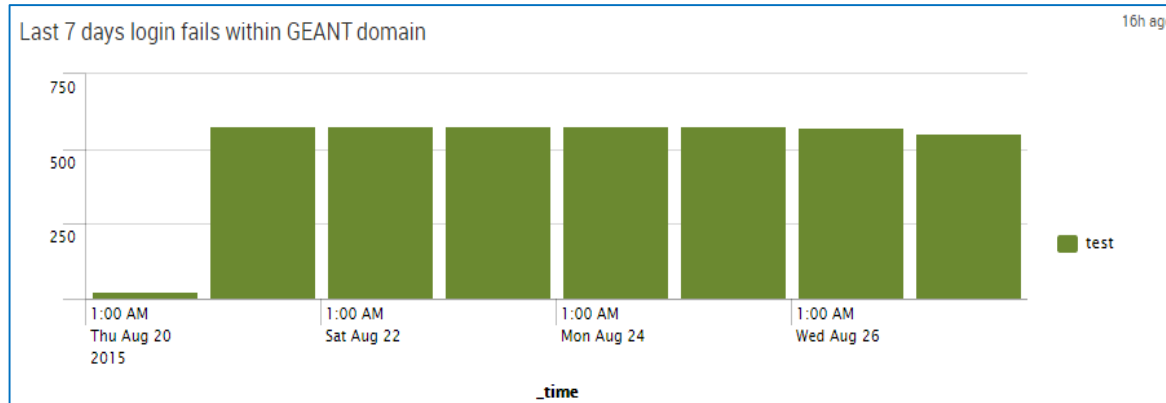


Others include:

BGP peering attempts
SNMP unauthorized access

.....

Linux hosts dashboard

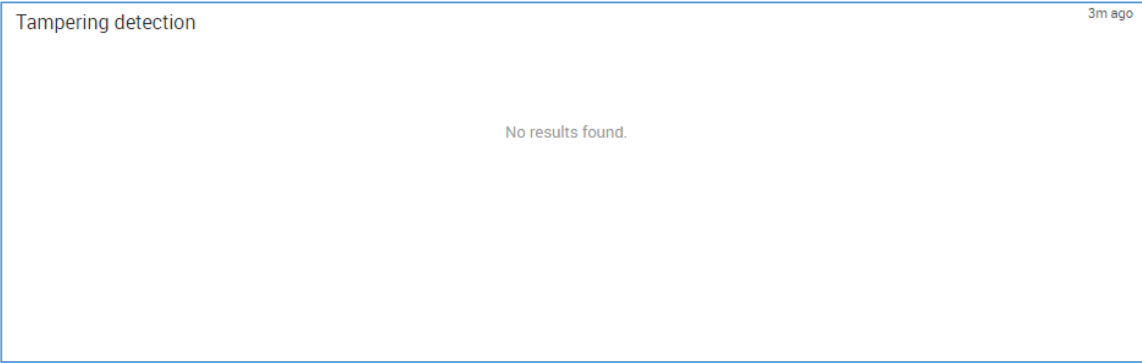
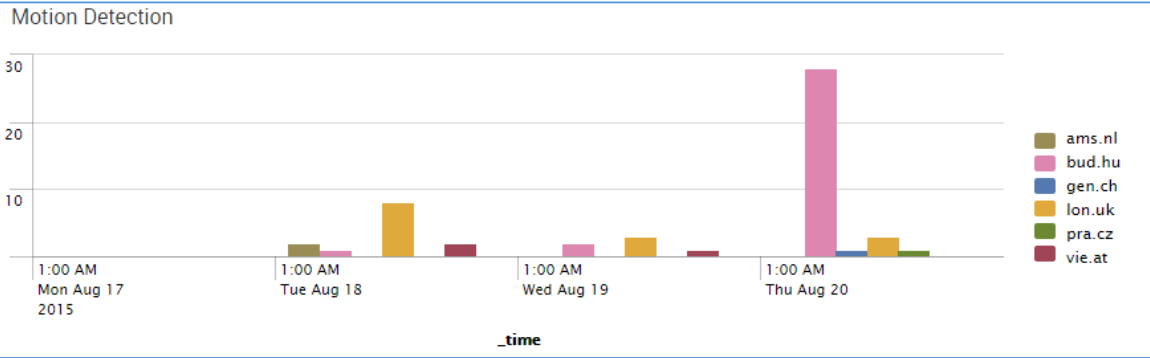


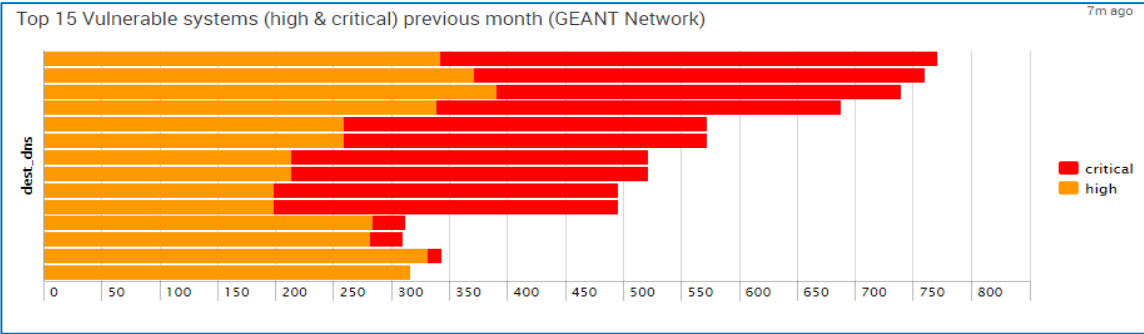
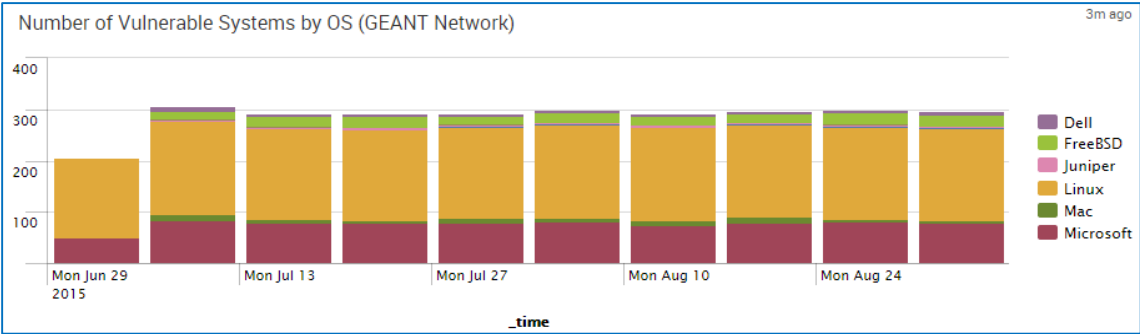
Others include:

Login fails outside GEANT domain
User addition/deletion

.....

Camera Dashboard





Others include:

Total number of vulnerabilities by severity
New alive or dead hosts

.....

Do we have complete visibility?

- Linux logs ✓
- Router/switch logs ✓
- Camera logs ✓
- Nessus report logs ✓
- Windows logs ✗



Plan to accommodate Windows logs

- How many more logs from Windows? → **2.2 GB/day → 3.2 GB/day total**
- Is the HDD space suffice? What about I/O speed? → **OK**
- Is RAM and CPU suffice for processing? → **Small upgrades**
- Is current vmNIC able to cope with the volume? → **OK**
- What additional software is required to ship the logs to Splunk? → **Splunk UF**
- How many resources for deployment? → **15 days**
- What is the price for license upgrade and recurring costs? → **£9,660.00 + £3,252.00 for 5 GB/day**

- Another upgrade in 5 years
- NetFlow? Another upgrade?

... still confined by price per volume

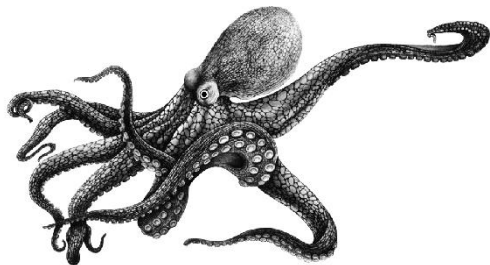


What are we interested in?

- Hardware/software requirements (RAM, CPU)
- Level of skill required for managing/configuring it
- Recurring costs
- Scalability/redundancy/search speed
- Alerting
- Integration with existing tools

Most importantly: do we maintain existing Splunk functionality and build more on top of that, or lose?

Open Source Logging Tools





**£5,000 / node – Gold Support
(~6,882 EUROS)**



**£4,100 / node – Gold Support
(~5,643 EUROS)**

Can ELK/Graylog2 substitute Splunk







GÉANT

ASSOCIATION

Networking • Services • People

Thank you & happy logging!

Security@geant.org

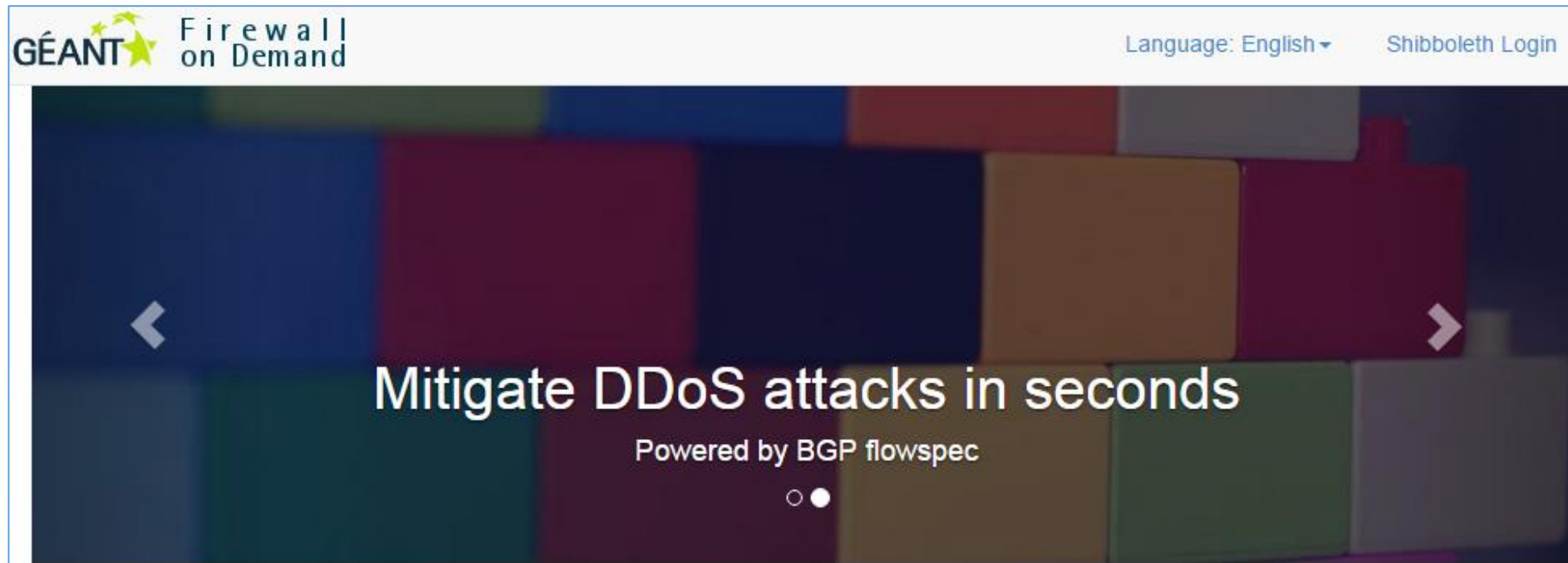
Evangelos.Spatharas@geant.org

Firewall on Demand - Update

Currently → Pilot (24th Aug. 2015 – 23rd Oct. 2015) | 2 NRENs

Next → KPIs review and tweaking based on NREN needs

Next after Next → App enhancements



Interested on participating in the pilot?? → security@geant.org