**POC**

* JSON
* GELF
* [Rsyslog docs]
* Graylogs docs

**Prod**

* VRT/ET payant choix
* Suricata docs
* Suricata/graylog optimisation (#paquets dropped suricata)
* Security debian, graylog (TLS…)
* LDAP
* Logs retention
* Alerting/reporting

**Finalisation**

* #paquets dropped par NIC/OS
* Docs kernel
* Kernel optimisation : NAPI ? PF\_ring ? Load balancing des IRQs ? #IRQ

**Externe**

C

Foo pointeur de structure

Foo->x idem (\*foo).x

Docs

Merger Bash

Merger Kernel – imprimer code kernel

Questions

* Avec ou sans Sagan, Aanval ou OSSIM en amont ou aval.
* Appache kafka ou rabbitMQ load balancer si graylog ne peut pas suivre ?