**POC**

* ~~JSON~~
* ~~GELF~~
* ~~[Rsyslog docs]~~
* ~~Graylogs docs~~
* ~~Real time~~ + dashboard

**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 Kiennert ou perso

* Avec ou sans Sagan, Aanval ou OSSIM en amont ou aval.
* Appache kafka ou rabbitMQ load balancer si graylog ne peut pas suivre ?
* Résolution du https de bout en bout.
* OS refragmente (IP – TCP)? ou Suricata ?
* Liste des IPs atteignables sur le site ?
* Administration de la machine physique hébergeant suricata ?SSH ?
* Liste des protocoles Euris.