**Niveau 1 : Alertes critiques avec trap Centreon**

* Grosse surcharge réseau
* Stream avec ports non courants dans l’infra
* Attaque applicative sur une IP connue
  + Bruteforce >20 en une minute
  + Echanges avec des IPs répudiées
  + Charge malsaine, injection SQL…
* Serveur initie une connexion de lui-même vers une IP non trusted

**Niveau 2 : Alertes Critiques sans trap Centreon**

* Scan de ports/services
* Une IP est souvent remontée par l’IDS (>20 alertes différentes par jour)

**Niveau 3 : alertes annexes**

* Mots de passes en clair
* Conformité des trames

Suspicion d’Attaques réussies ?