



# Détection d'attaques DDoS dans les réseaux

Gilles Roudiere

► **To cite this version:**

Gilles Roudiere. Détection d'attaques DDoS dans les réseaux. Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, May 2017, Grenoble, France. 2017. <hal-01528725>

**HAL Id: hal-01528725**

**<https://hal.laas.fr/hal-01528725>**

Submitted on 29 May 2017

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

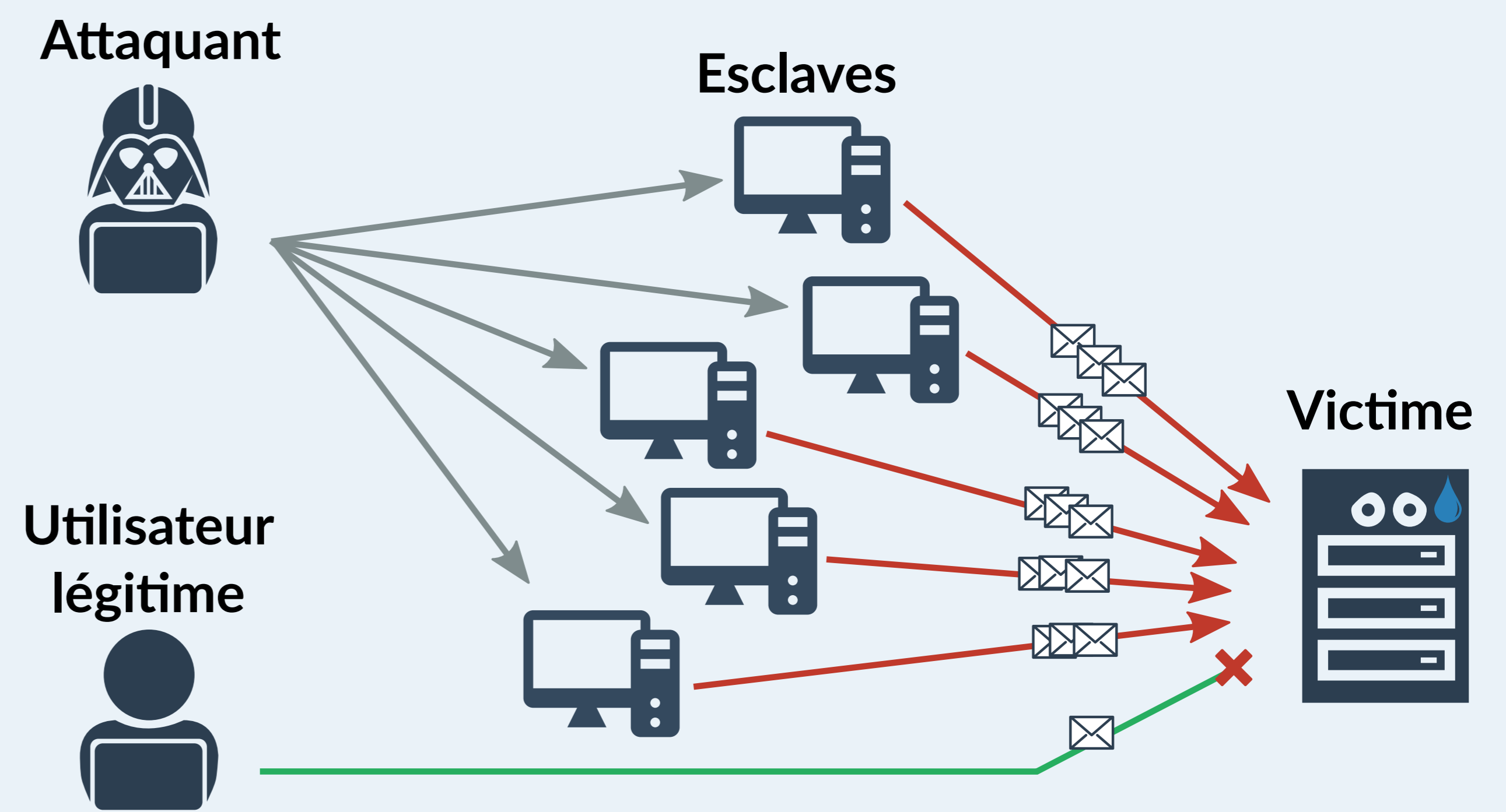
## Contexte

### Attaques par Déni de Service Distribuées (DDoS)

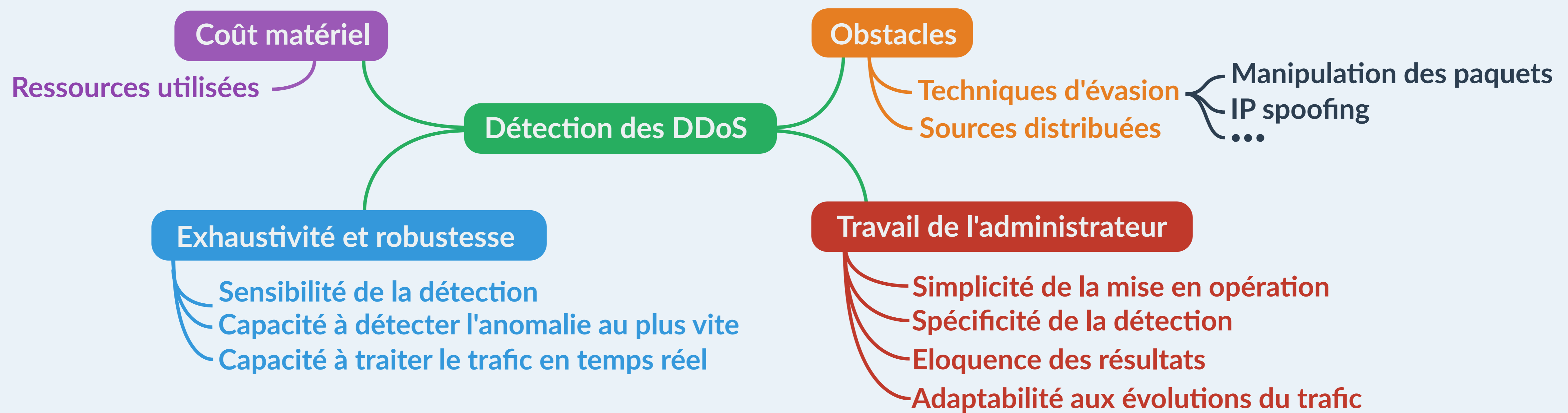
= Un grand nombre de machines envoient des requêtes parasites à un système cible, l'empêchant de répondre aux requêtes légitimes.

**Coûteuses** \$2.5 millions en moyenne par attaque, 63% des entreprises estiment le coût de l'indisponibilité de leurs services à plus de \$100.000 par heure.

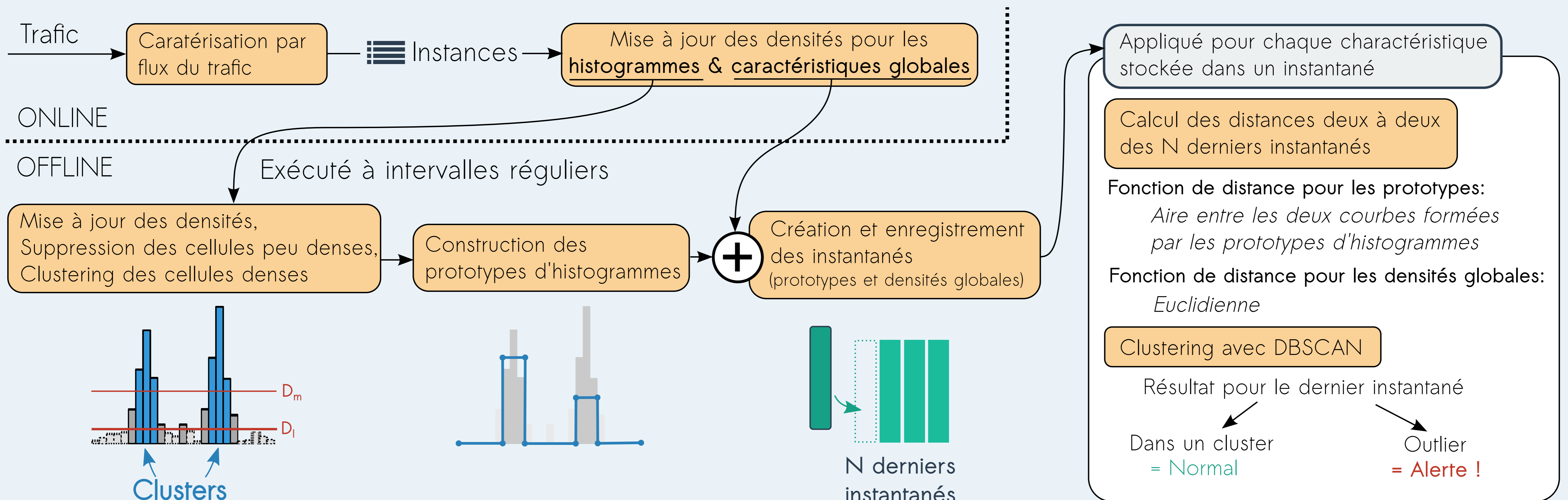
**Nombreuses** 84% des entreprises en ont subi au moins une en 2016.  
 (Enquête réalisée auprès de 1010 organisations. Source : Neustar, 2017)



## Problématique



## AATAC (Autonomous Algorithm for Traffic Anomalies Characterization)



- Division du traitement en deux parties = détection **temps réel**, nécessitant peu de ressources de calcul,
- Des instantanés du trafic produits régulièrement :
  - Utilisant des histogrammes, qui sont graphiquement **simples à interpréter** (et plus parlants que l'entropie par exemple),
  - Formant une vue dynamique du trafic, **simplifiant la phase d'analyse**.

## Expérimentations

**SynthONTS** : 13 anomalies générées dans un ensemble de traces réelles. (Les travaux sur ce jeu de données continuent avec une extension en cours de la trace et du nombre d'anomalies synthétiques qu'il contient.)

**Taux de vrais positifs** : 0.83  
**Taux de faux positifs** : 0.0013

**Traces réelles** : traces capturées à l'entrée d'un réseau d'entreprise (essentiellement du trafic web, contenant deux DDoS).

N	Online (Temps de calcul en s pour 1s de trafic)	Offline (Temps de calcul en ms)
100	0.20	0.029
1000	0.20	0.028
5000	0.21	0.030

## Analyse des résultats : exemple avec un prototype d'histogramme

