Apprentissage adverse et algorithmes de détection d'évènements : une première typologie

Olivier de Casanove, Florence Sèdes

▶ **To cite this version:**

Olivier de Casanove, Florence Sèdes. Apprentissage adverse et algorithmes de détection d'évènements : une première typologie. Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2022), May 2022, Chambon-Sur-Lac, France. 2022. hal-03668829

HAL Id: hal-03668829
https://hal.science/hal-03668829

Submitted on 16 May 2022

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.

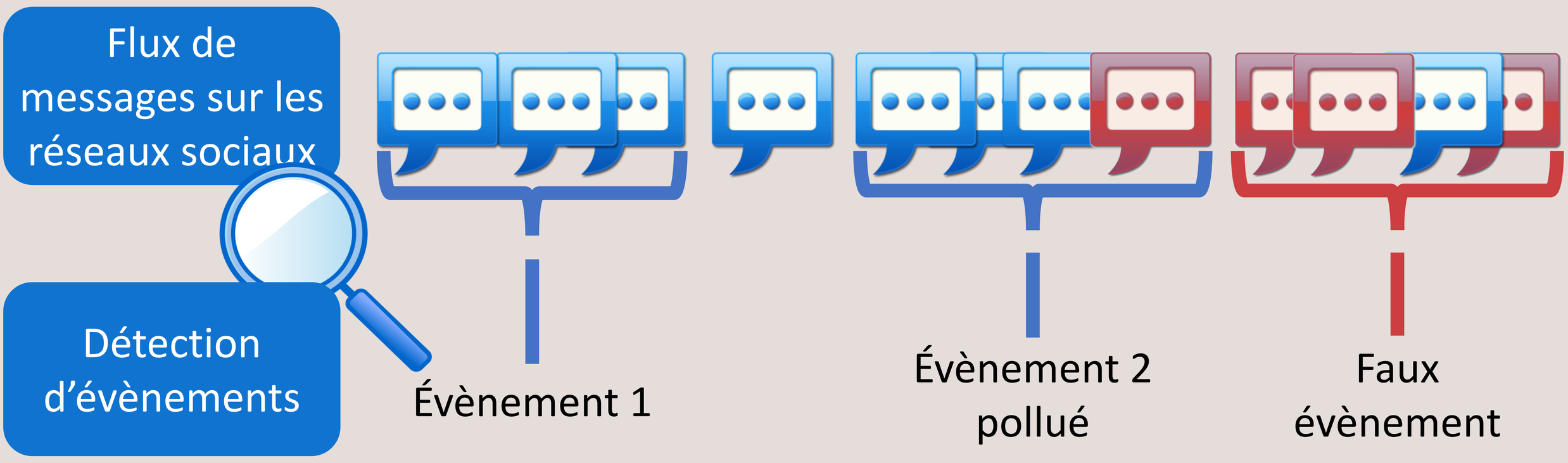
Institut de Recherche en Informatique de Toulouse

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université de Toulouse

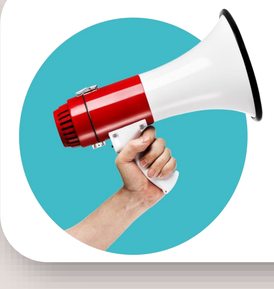
Apprentissage adverse et algorithmes de détection d'évènements - une première typologie -

Olivier de Casanove, IRIT
Université Toulouse III – Paul Sabatier
olivier.decasanove@irit.fr

Florence Sèdes, IRIT
Université Toulouse III – Paul Sabatier
florence.sedes@irit.fr



Qui attaque ?



LE SPAMMER
- Polluer le flux d'information
- Promouvoir des contenus

L'ADVERSAIRE
- Nuire spécifiquement à la détection

LE TROLL
- Propager des rumeurs
- Désinformer

Quelles attaques ?

MODIFICATION

CREATION

DISPERSION