Journées Cloud 2018

inventeurs du monde numérique

MYRIADS

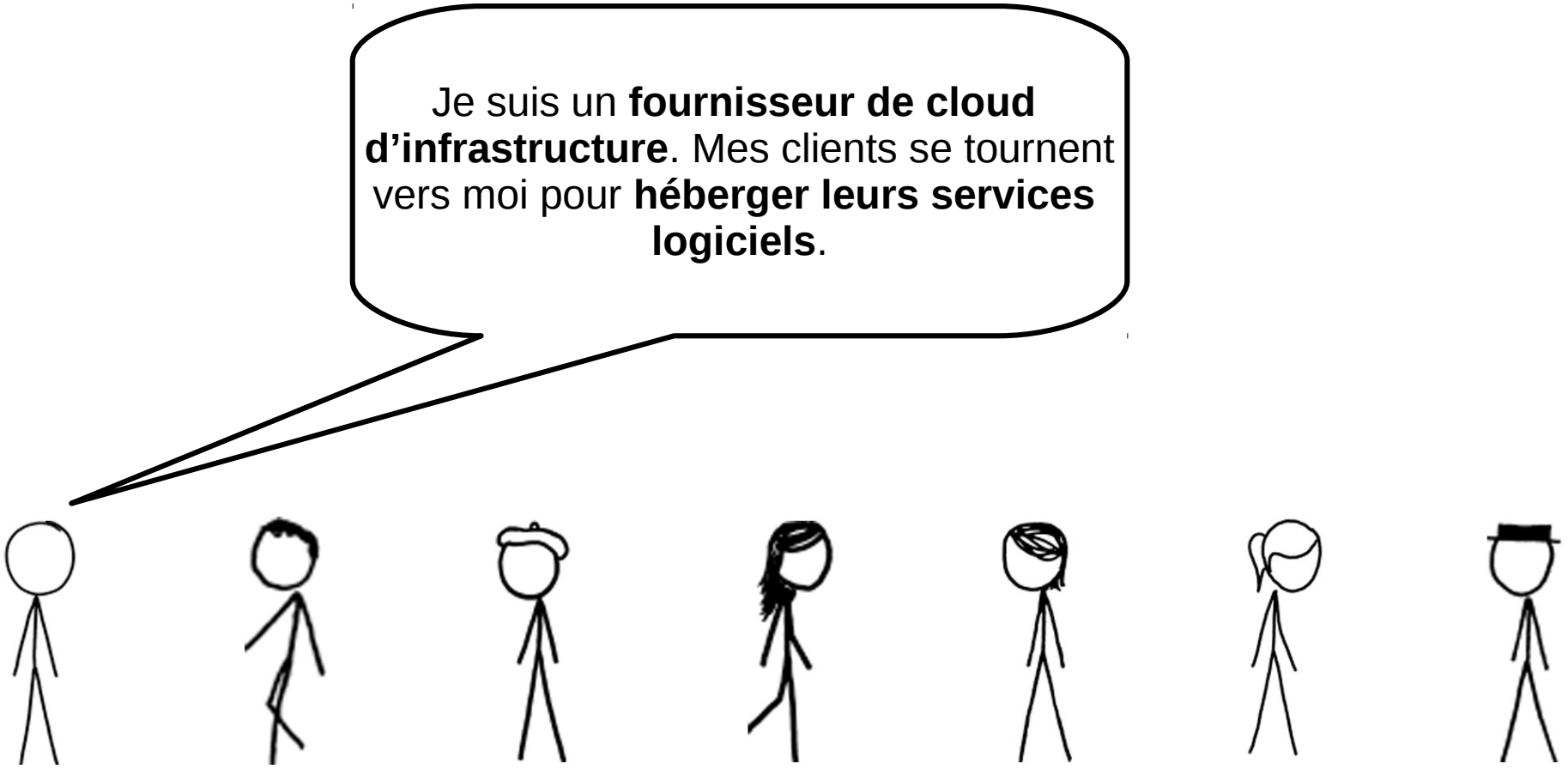
Mesurer et prévenir l'évolution de la menace dans un cloud d'infrastructure

Clément Elbaz (Inria), Louis Rilling (DGA), Christine Morin (Inria)

Les acteurs de la sécurité du cloud

Crédit : xkcd.com

Les acteurs de la sécurité du cloud



Fournisseur de cloud

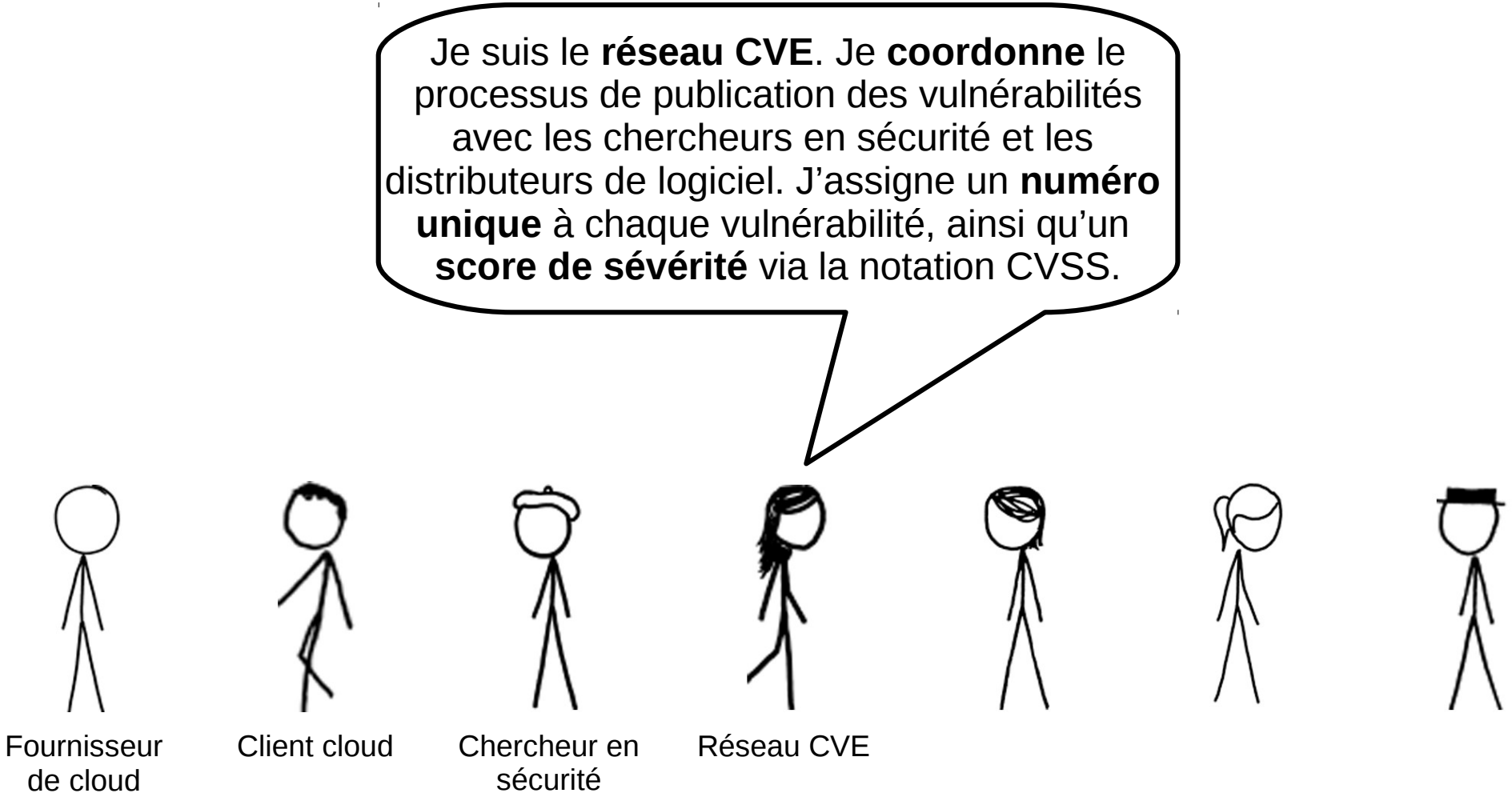
Les acteurs de la sécurité du cloud

Fournisseur de cloud

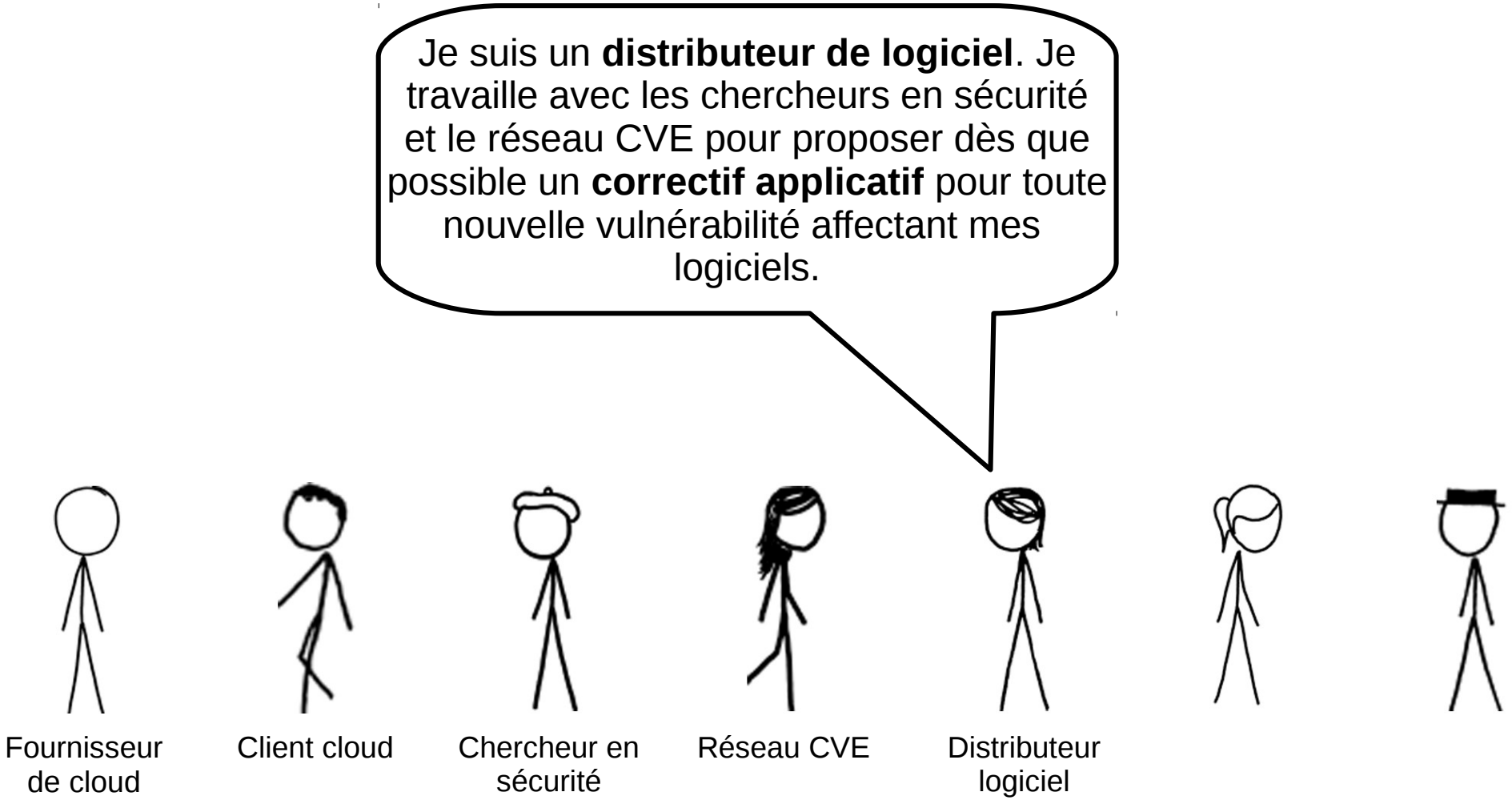
Client cloud

Les acteurs de la sécurité du cloud

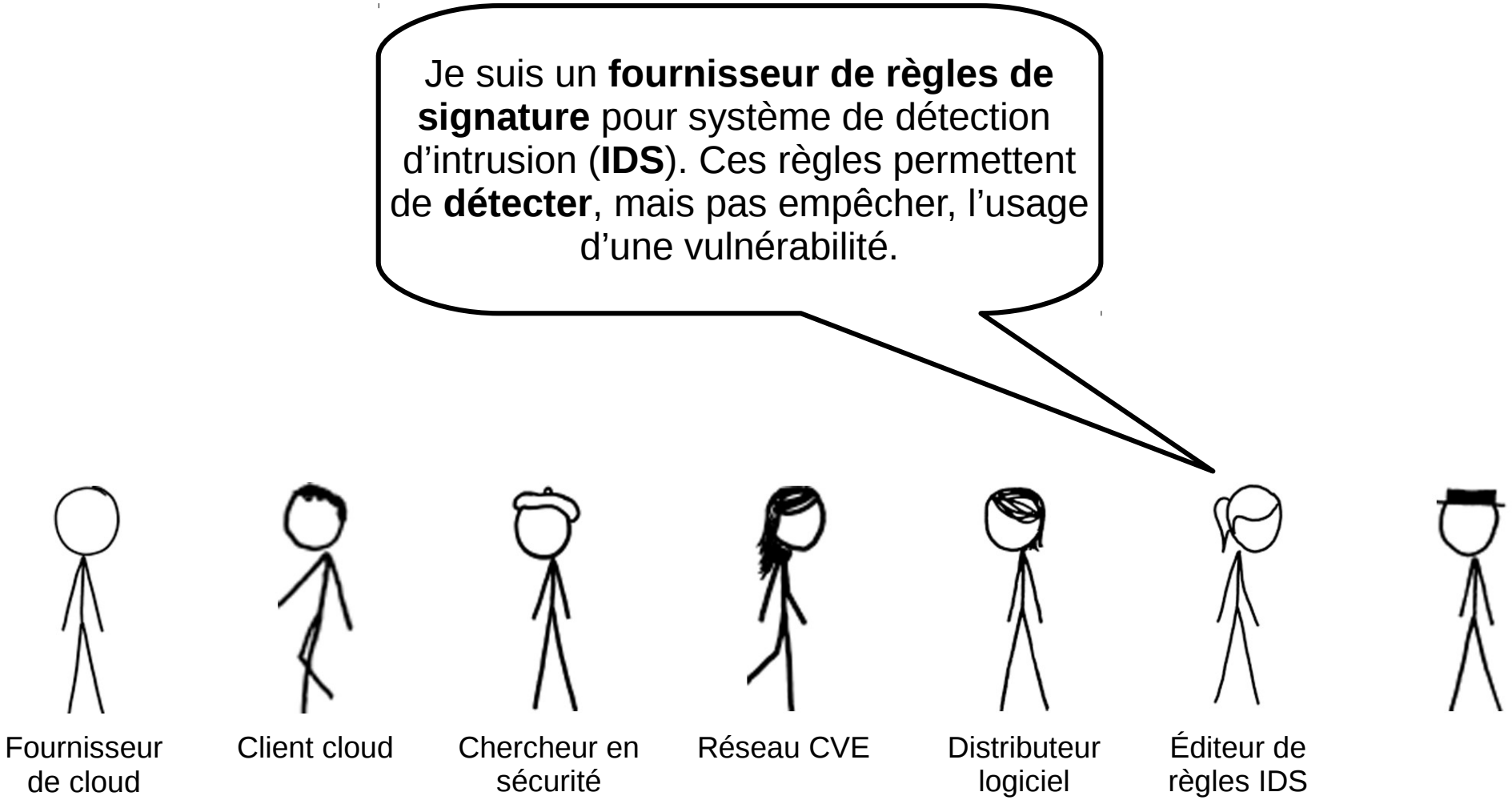
Les acteurs de la sécurité du cloud



Les acteurs de la sécurité du cloud



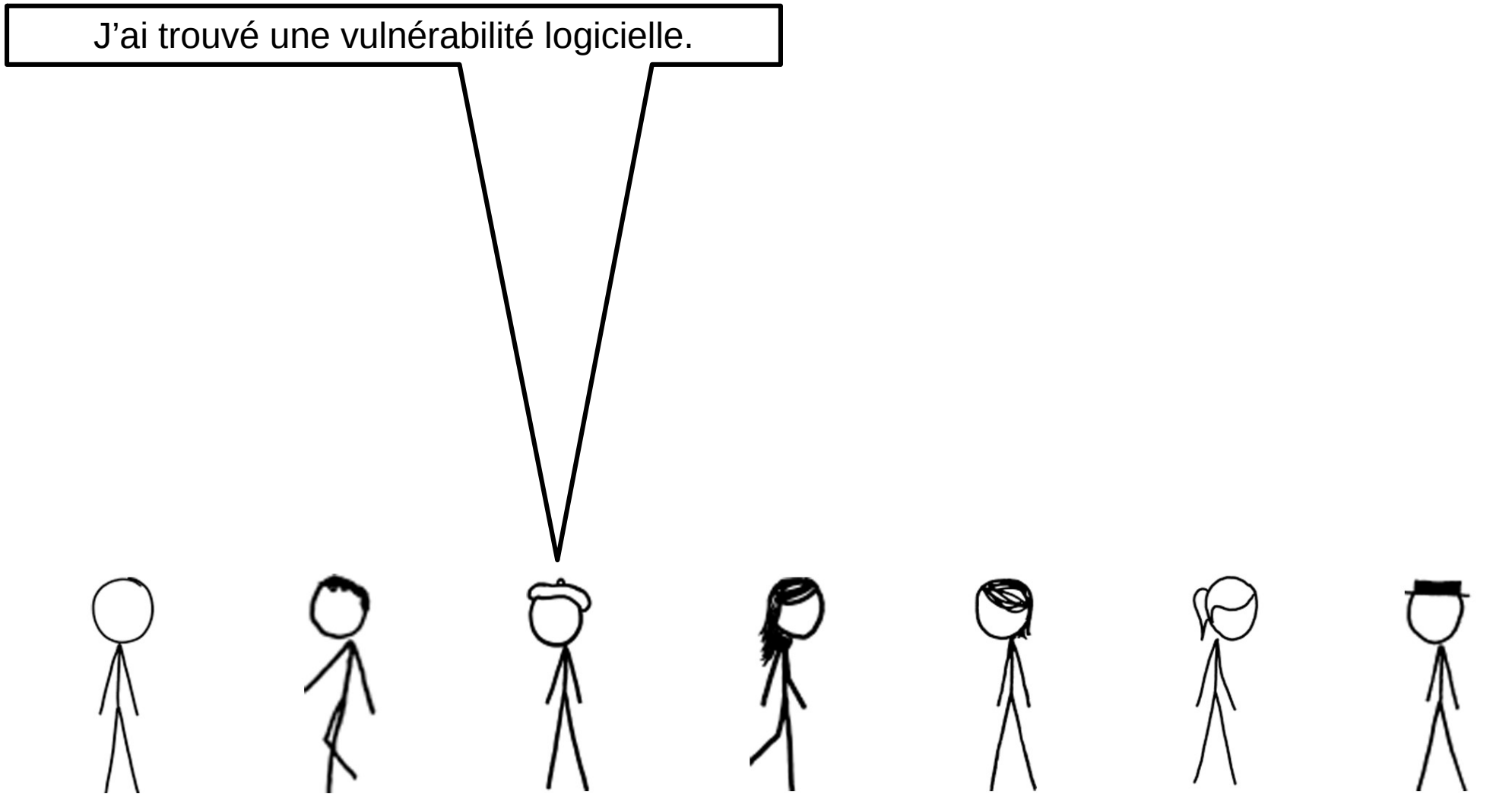
Les acteurs de la sécurité du cloud



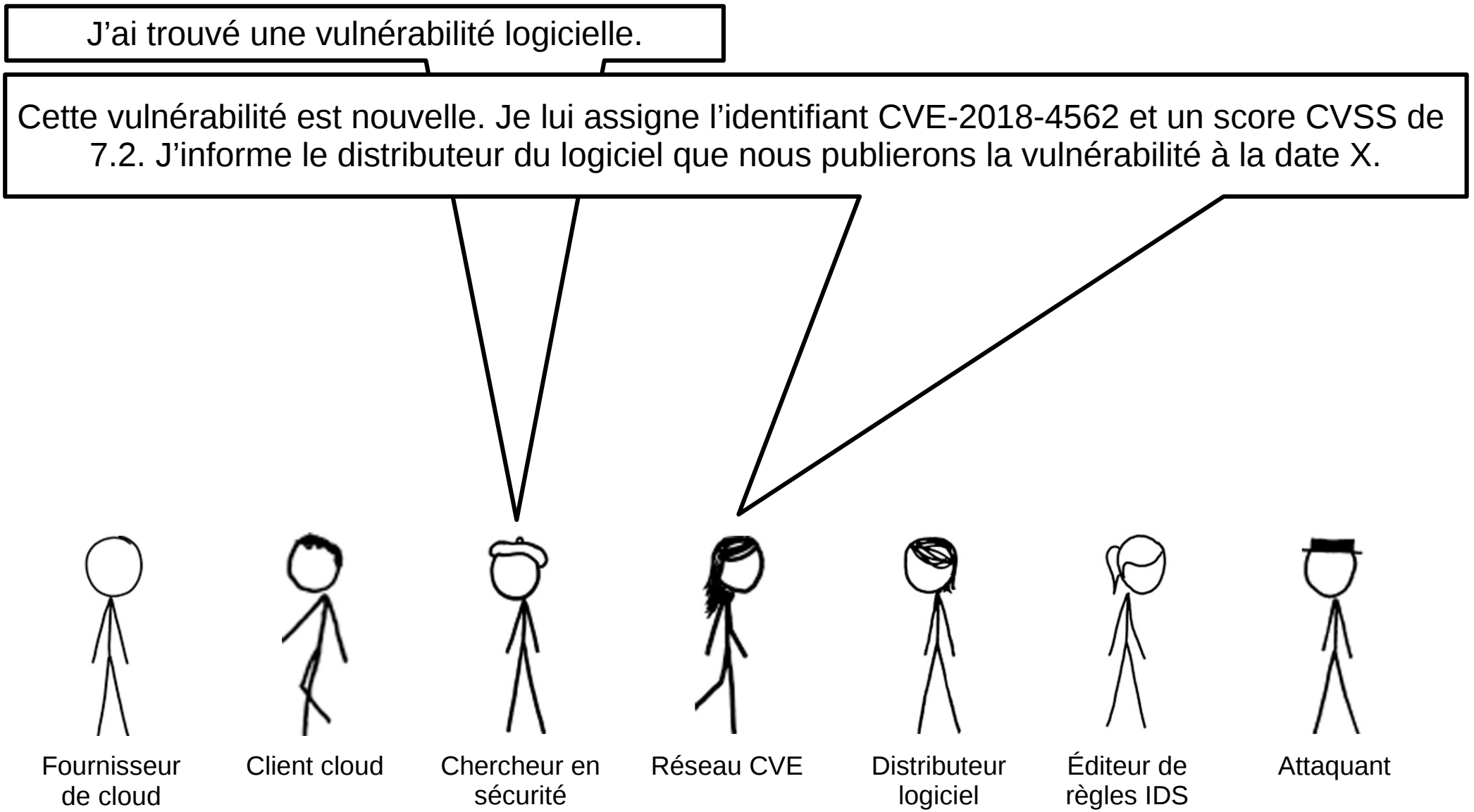
Les acteurs de la sécurité du cloud

Chaque nouvelle vulnérabilité
est une course contre la montre

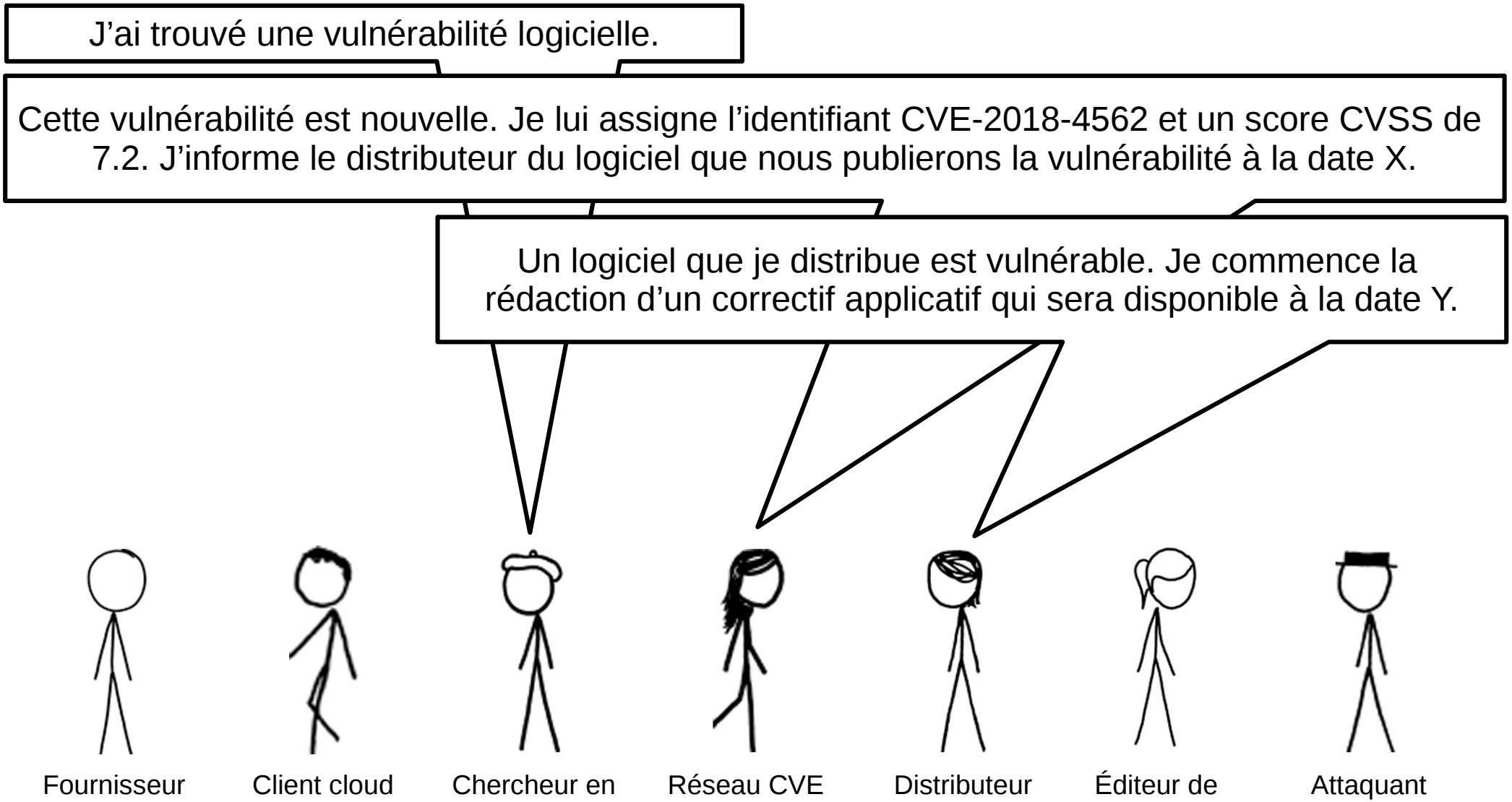
Nouvelle vulnérabilité = course contre la montre



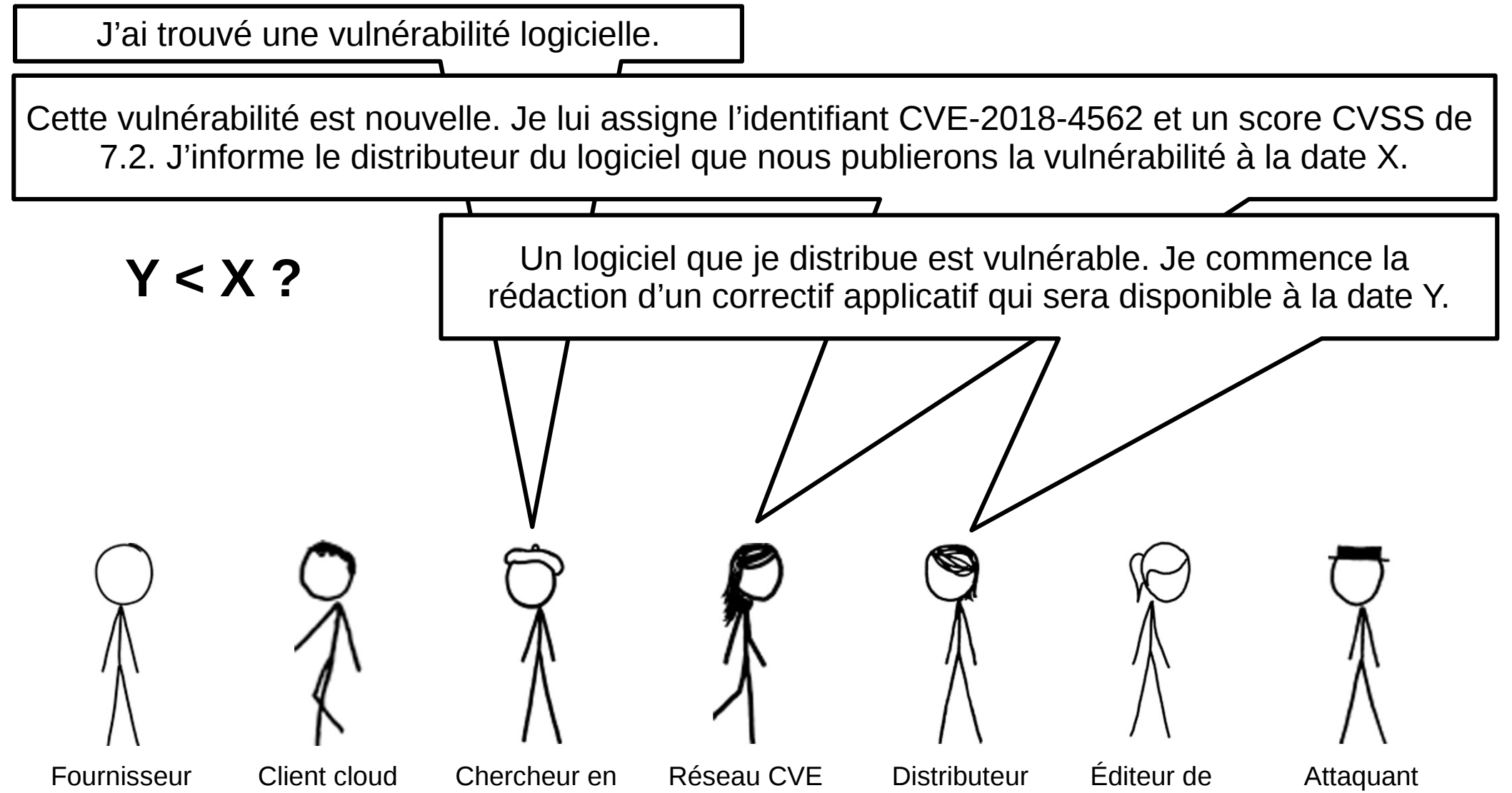
Nouvelle vulnérabilité = course contre la montre



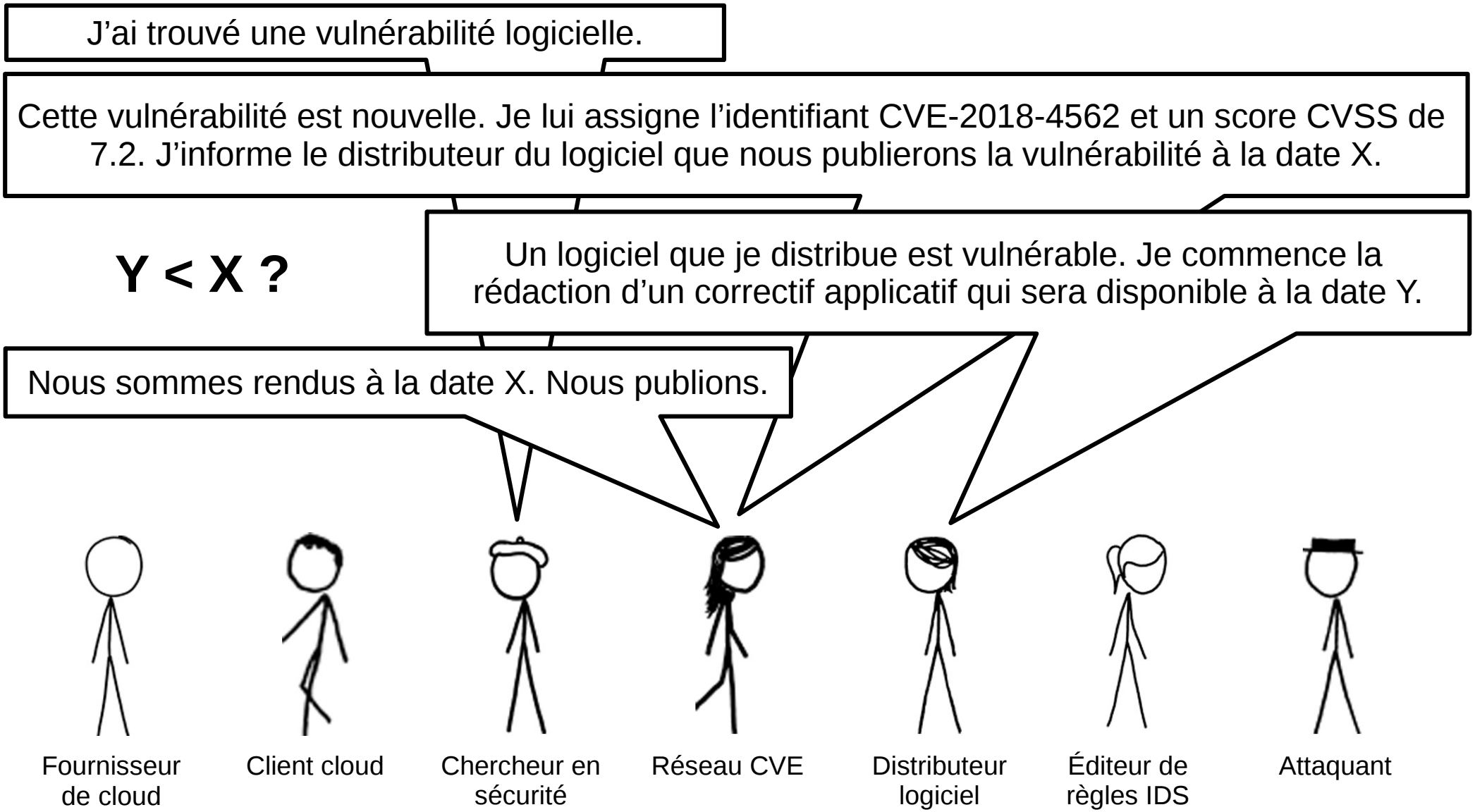
Nouvelle vulnérabilité = course contre la montre



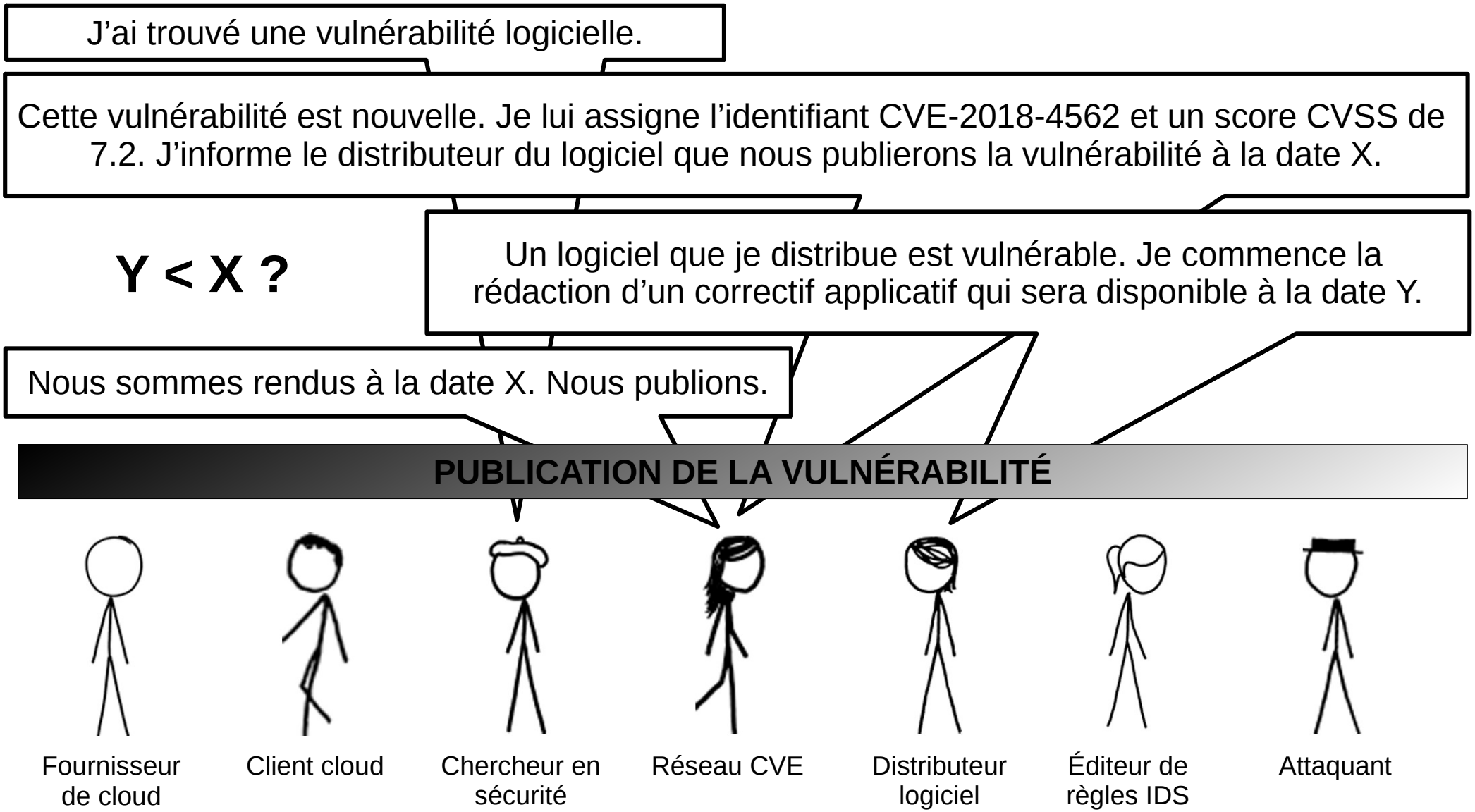
Nouvelle vulnérabilité = course contre la montre



Nouvelle vulnérabilité = course contre la montre



Nouvelle vulnérabilité = course contre la montre

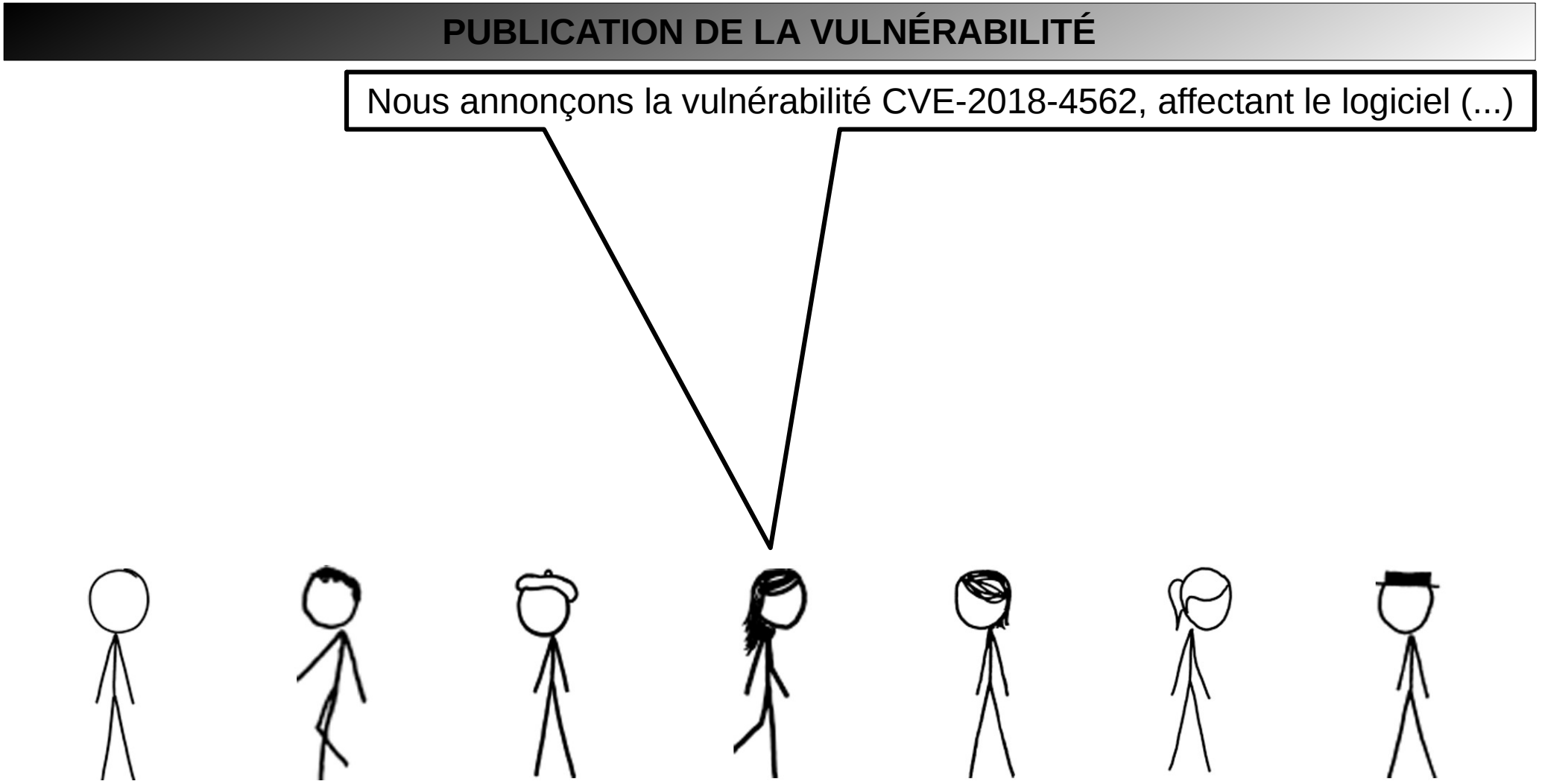


Nouvelle vulnérabilité = course contre la montre

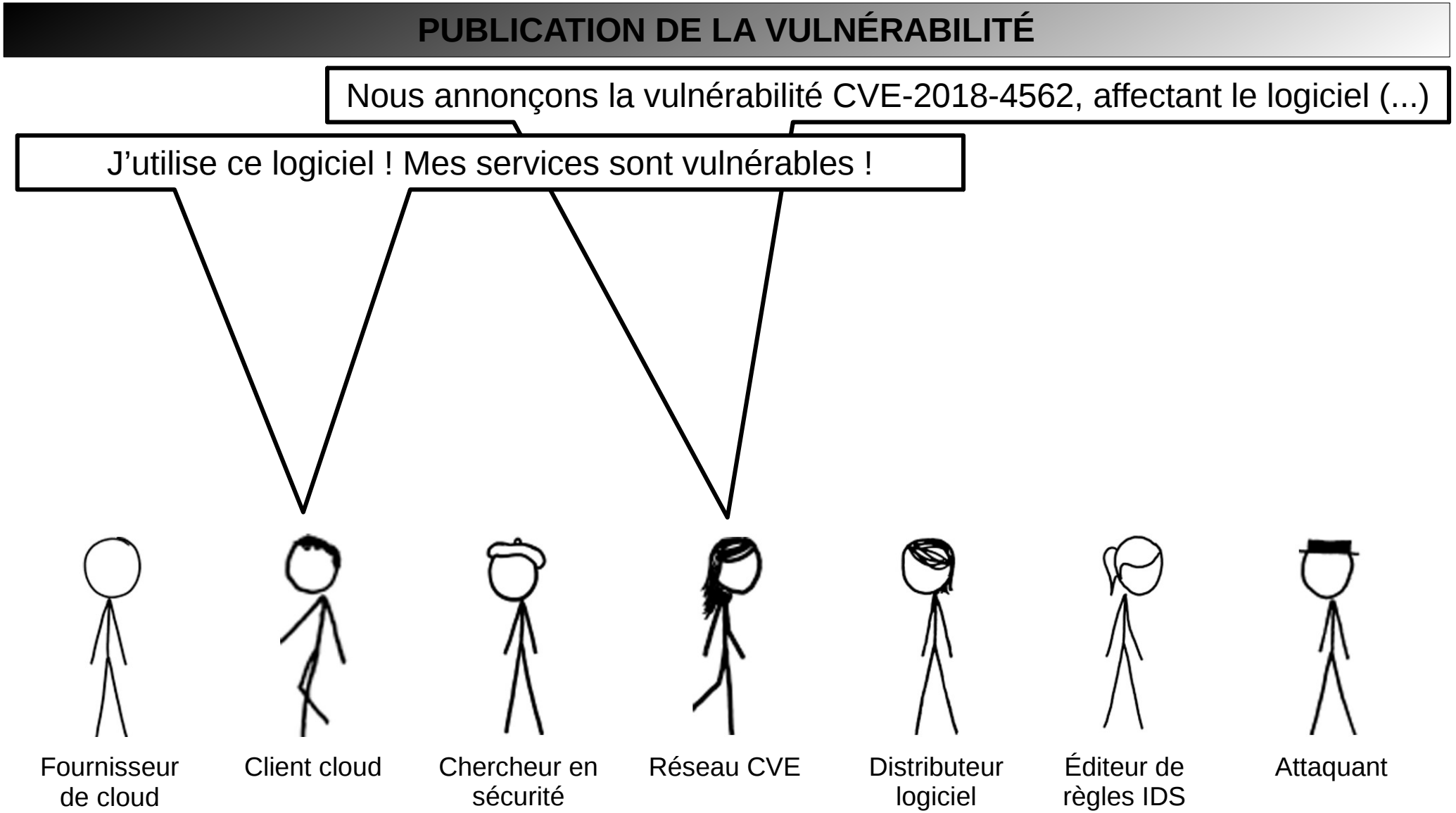
PUBLICATION DE LA VULNÉRABILITÉ

Fournisseur de cloud | Client cloud | Chercheur en sécurité | Réseau CVE | Distributeur logiciel | Éditeur de règles IDS | Attaquant

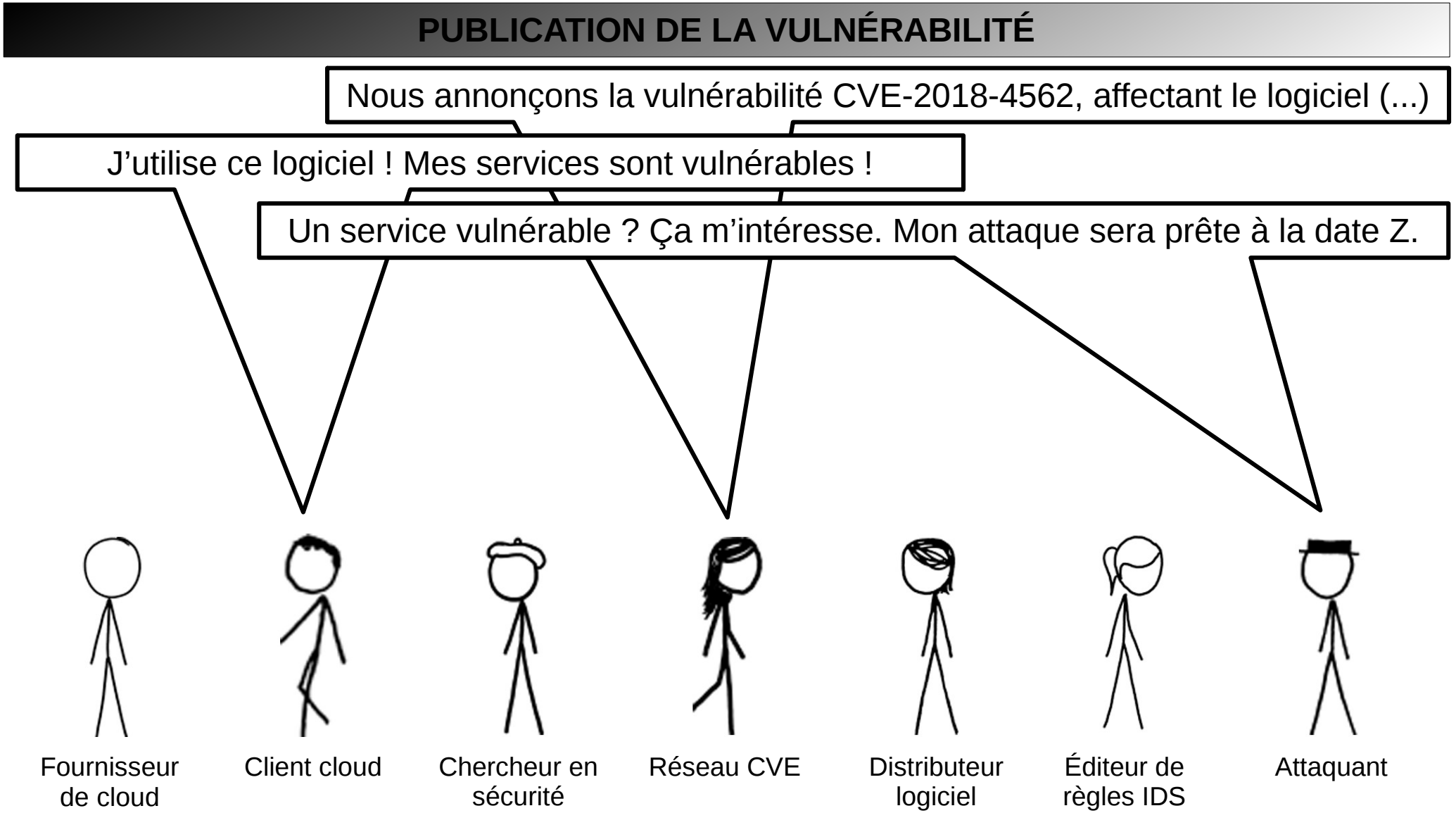
Nouvelle vulnérabilité = course contre la montre



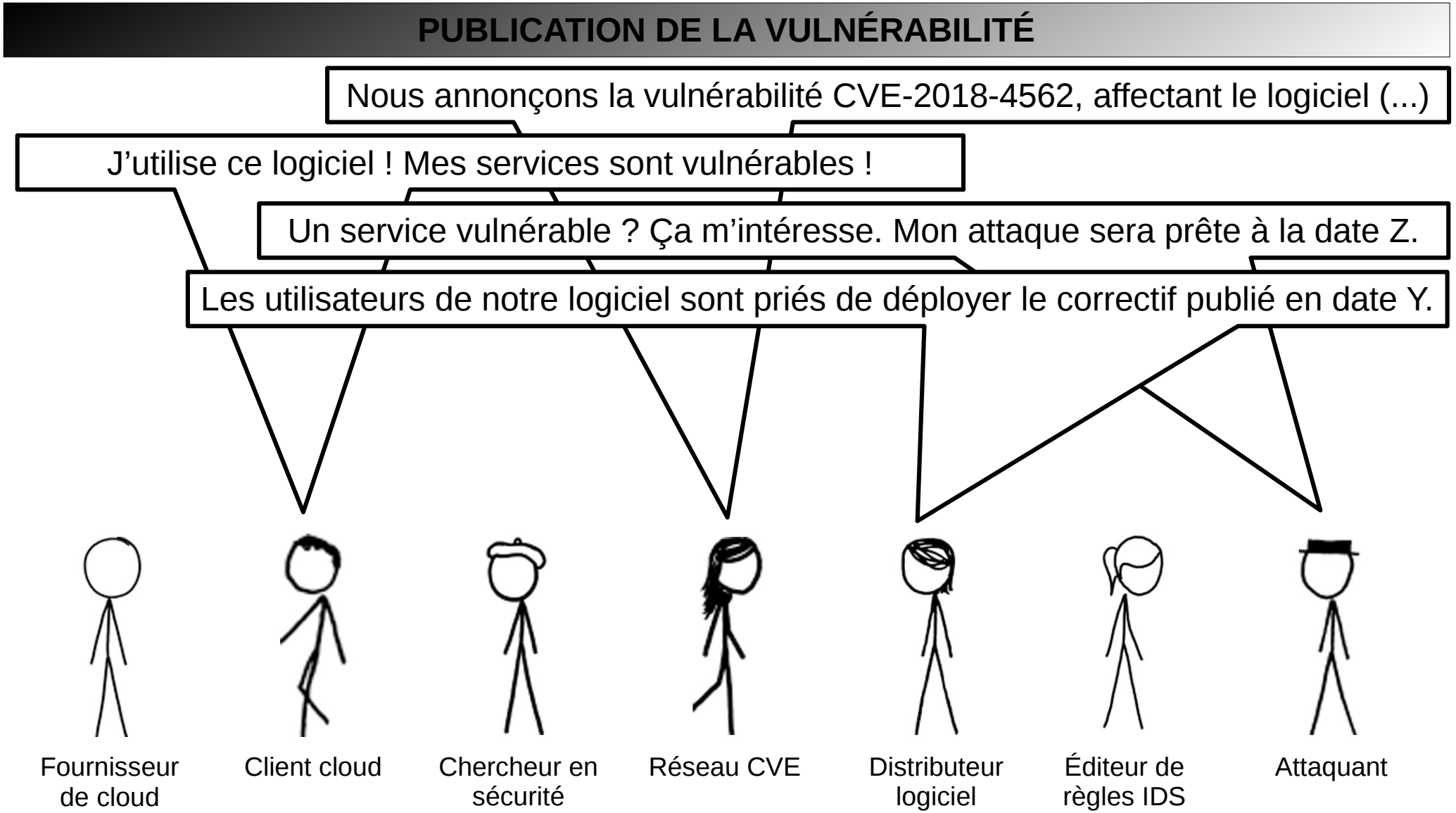
Nouvelle vulnérabilité = course contre la montre



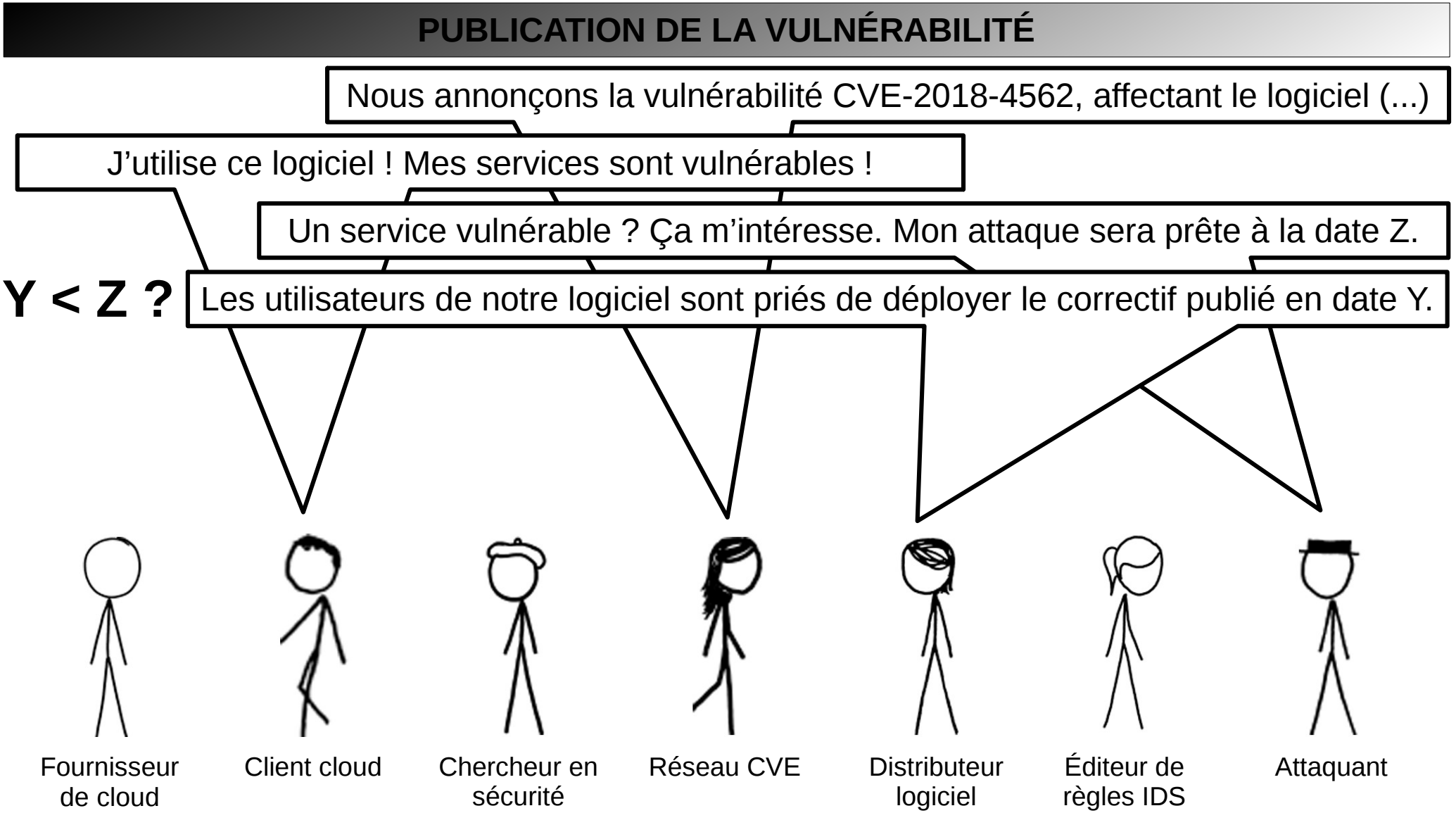
Nouvelle vulnérabilité = course contre la montre



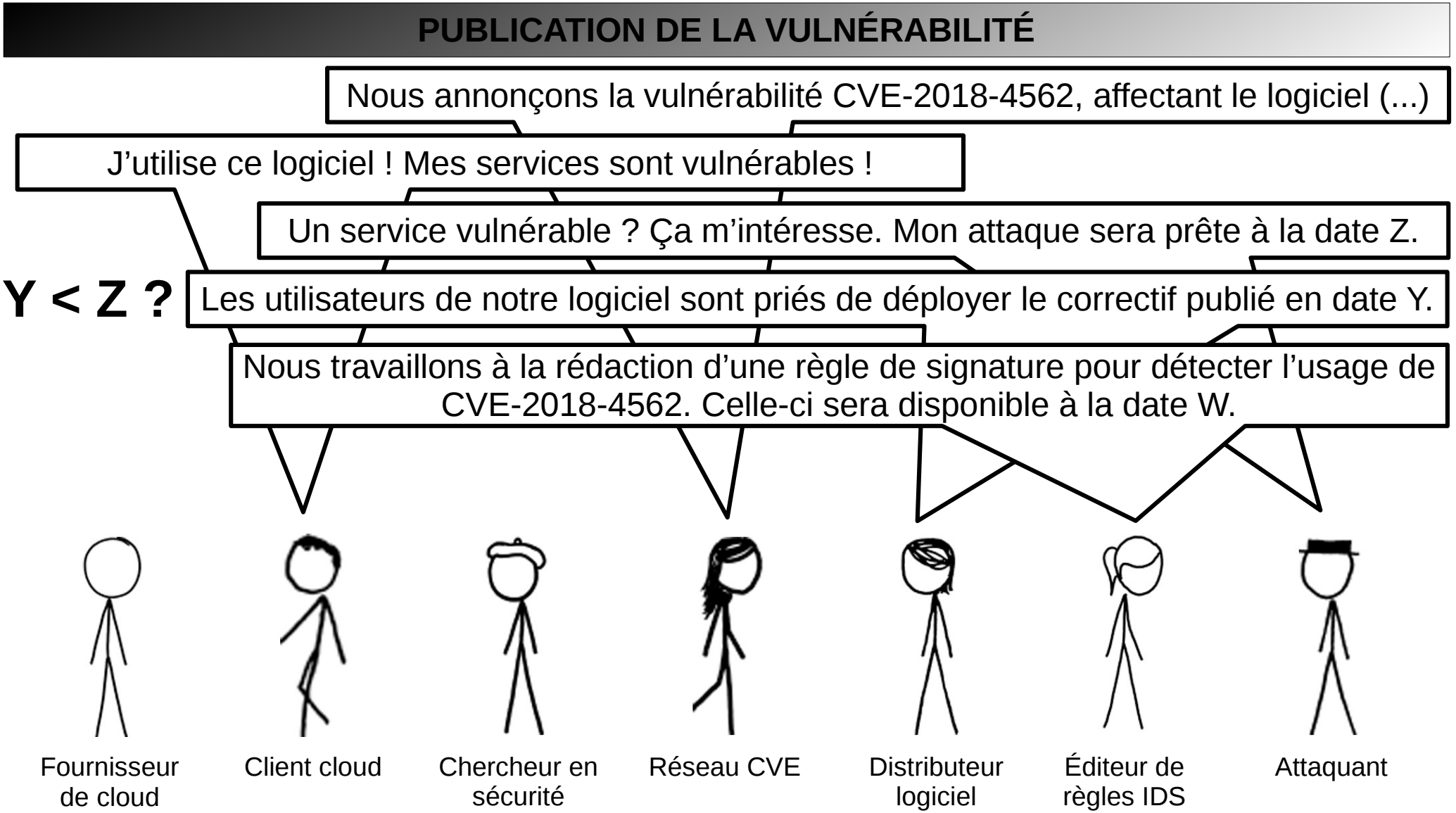
Nouvelle vulnérabilité = course contre la montre



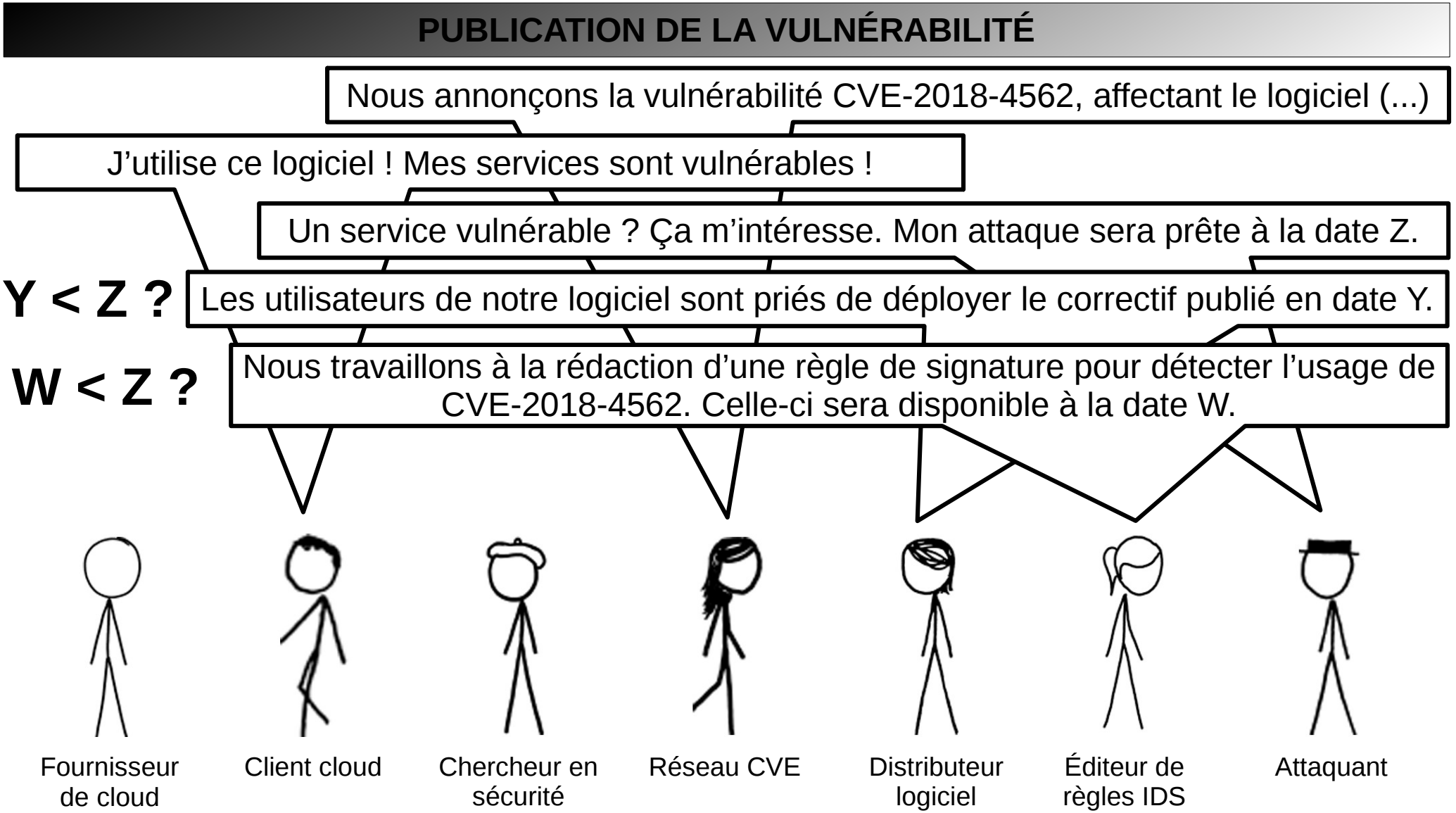
Nouvelle vulnérabilité = course contre la montre



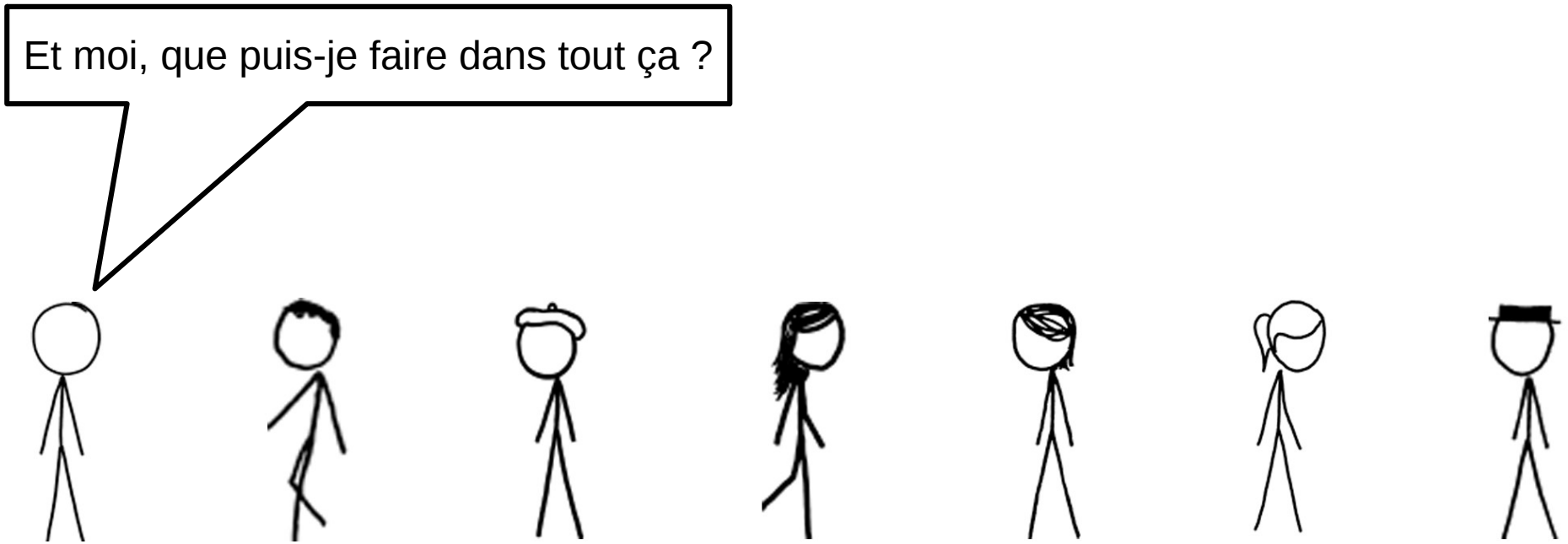
Nouvelle vulnérabilité = course contre la montre



Nouvelle vulnérabilité = course contre la montre

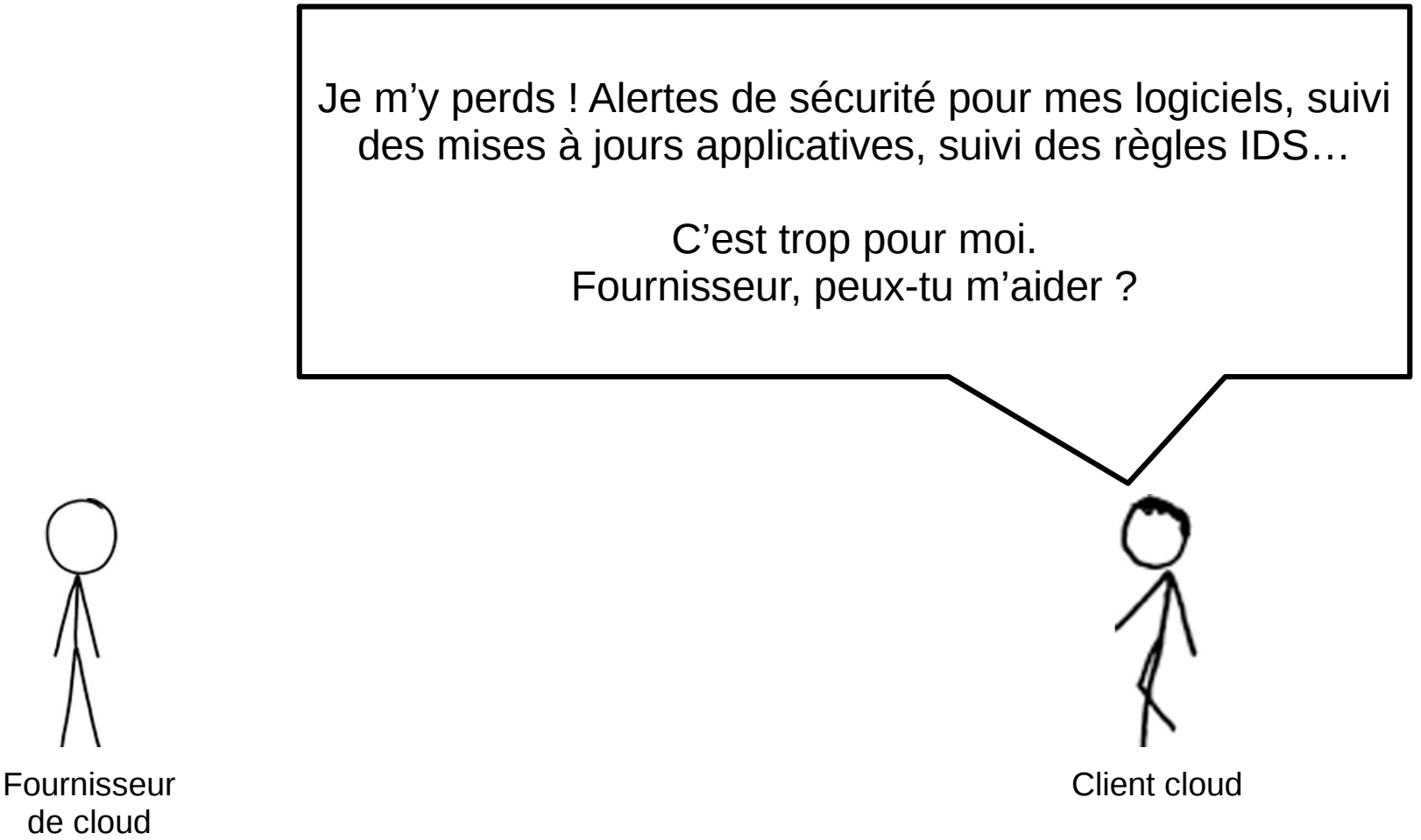


Nouvelle vulnérabilité = course contre la montre

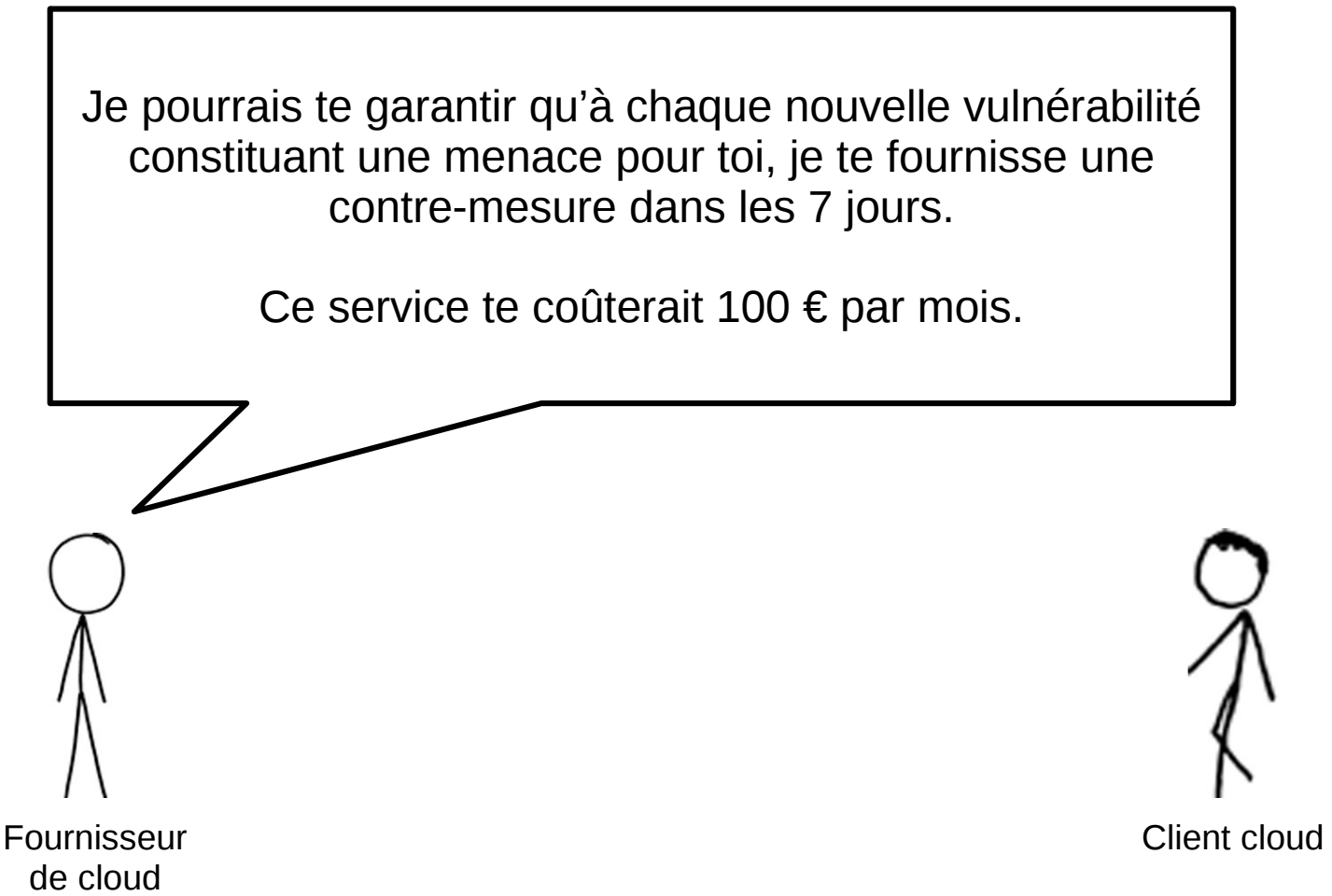


Conversation fictive entre un fournisseur de cloud et son client

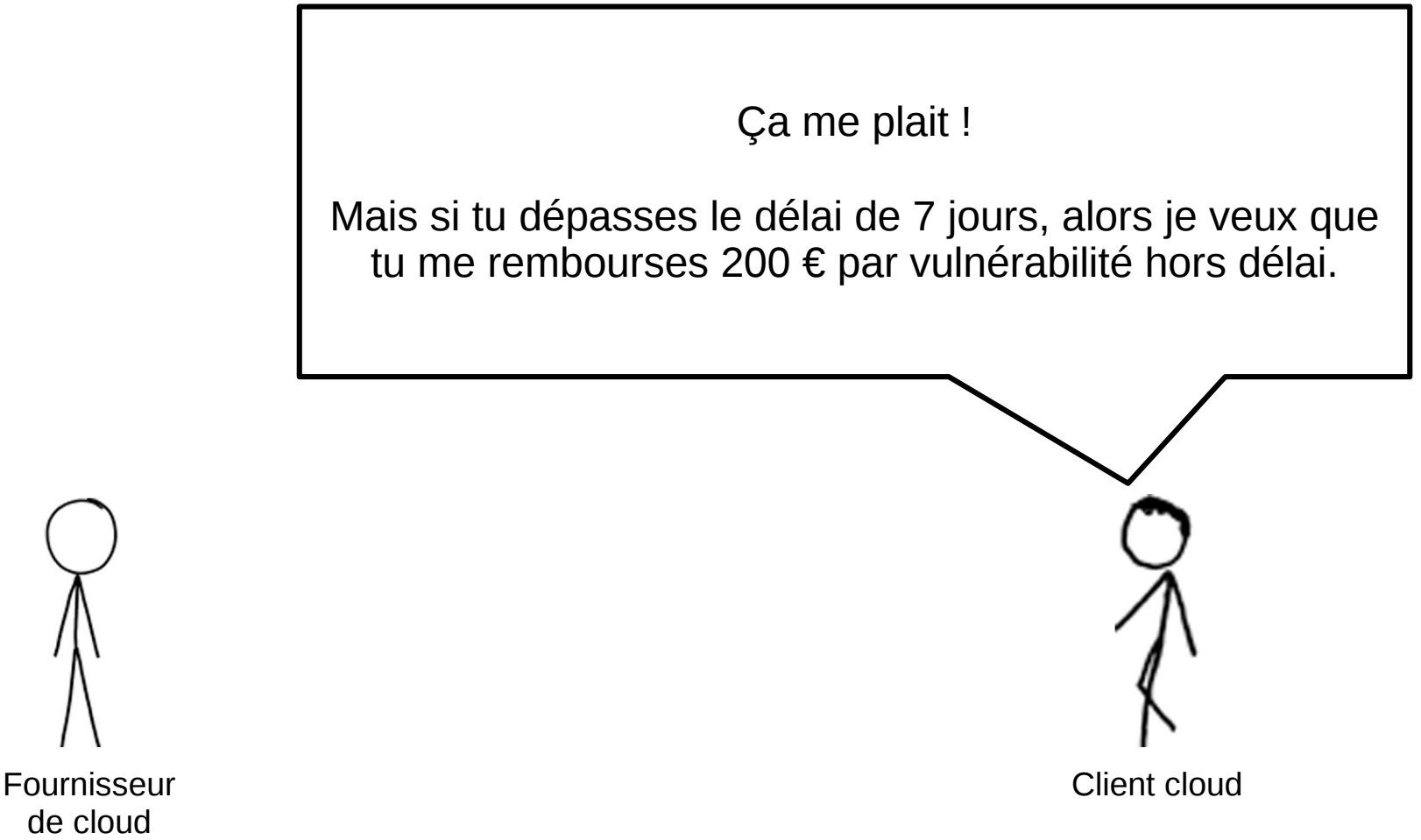
Conversation fictive



Conversation fictive



Conversation fictive



Conversation fictive

Fournisseur de cloud

Client cloud

Nos travaux

- Étude sur le cycle de vie des vulnérabilités et leurs contre-mesures

- Modèle économique et contractuel formalisant l'engagement d'un fournisseur de cloud auprès de ses clients à prendre en compte la publication de vulnérabilités

Nos travaux

- **Étude sur le cycle de vie des vulnérabilités et leurs contre-mesures**

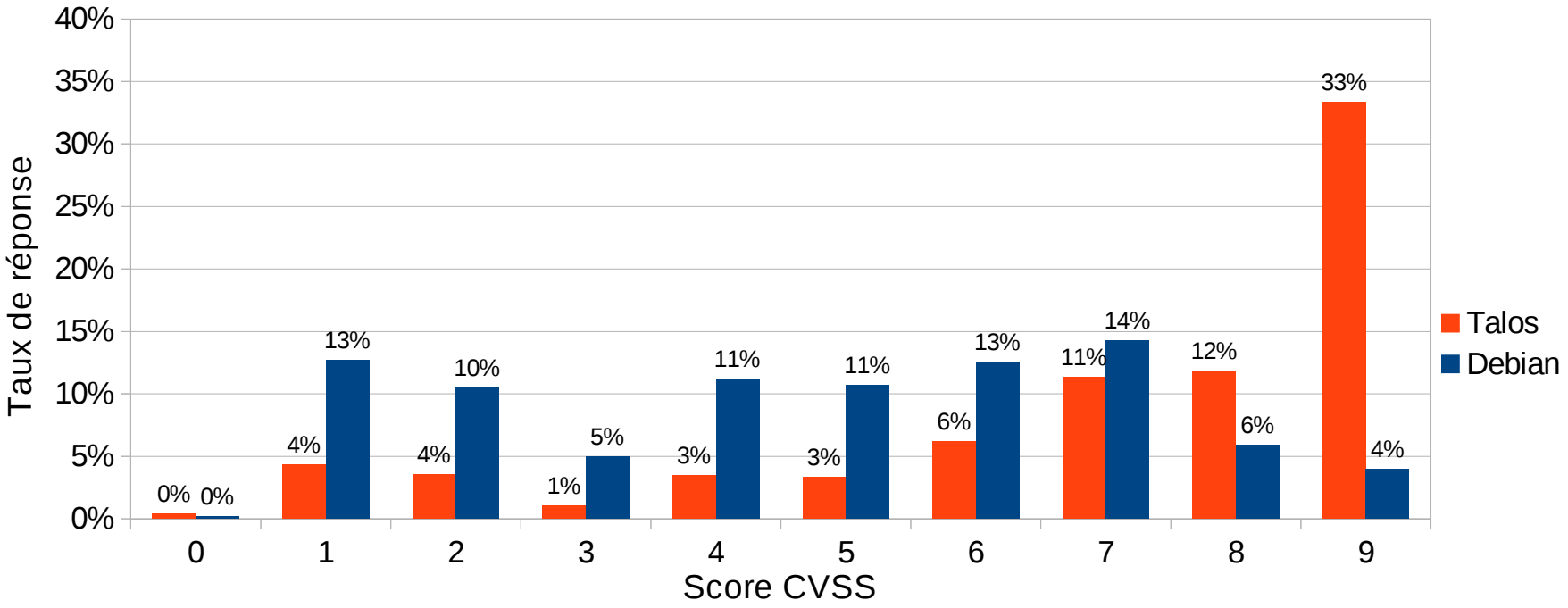
- Modèle économique et contractuel formalisant l'engagement d'un fournisseur de cloud auprès de ses clients à prendre en compte la publication de vulnérabilités

Cycle de vie des vulnérabilités

- Étude inédite
- Analyse des délais entre la publication d'une vulnérabilité et celle de ses contre-mesures
  - Correctifs applicatifs
    - Dépôt debian-security
  - Règles de signature pour système de détection d'intrusion (IDS)
    - Talos (jeu de règles officiel de Snort)
- 34 000 vulnérabilités publiées entre Juin 2014 et Octobre 2017

Résultats préliminaires

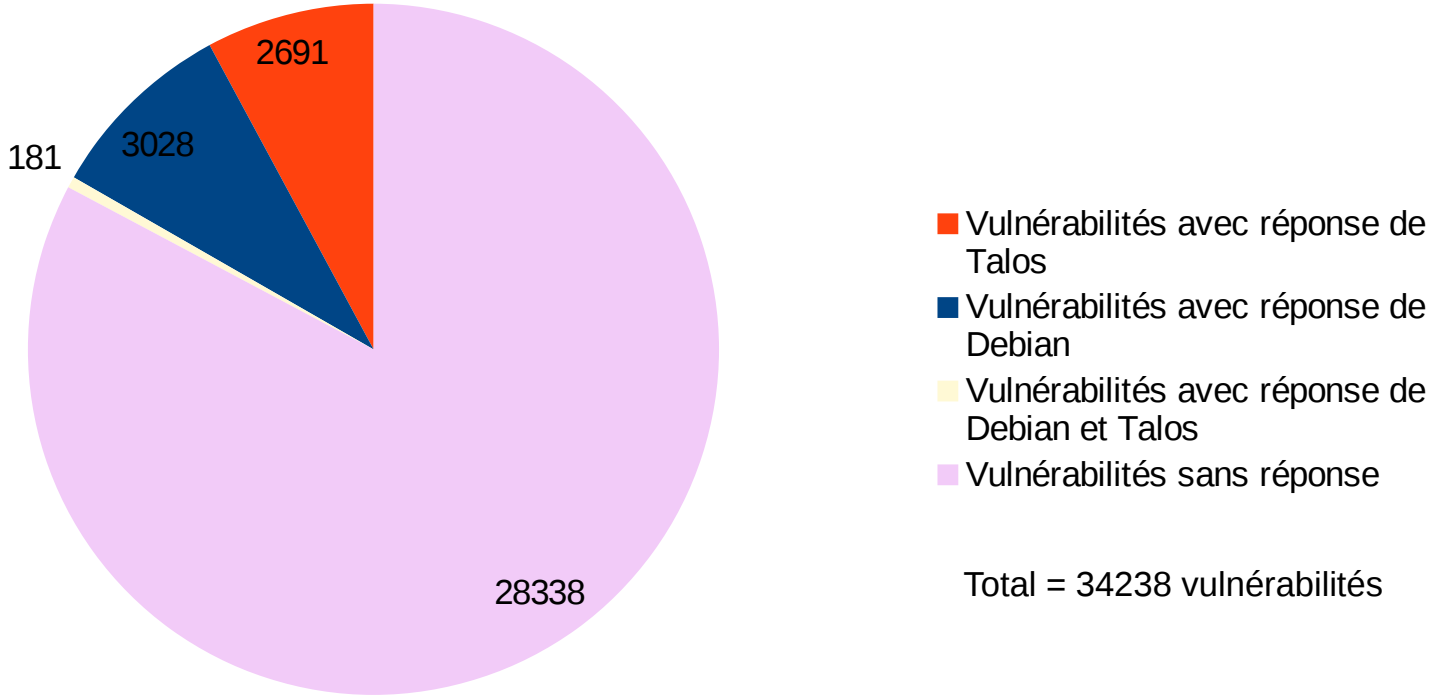
- Debian et Talos ne répondent pas aux mêmes vulnérabilités
  - Talos privilégie les vulnérabilités critiques (Score CVSS ≥ 9.0 sur 10.0)



Taux de réponse à une vulnérabilité en fonction de son score

Résultats préliminaires

- Talos et Debian répondent à peu de vulnérabilités
  - Seul **17.23 %** des vulnérabilités reçoivent une contre-mesure par Debian ou Talos

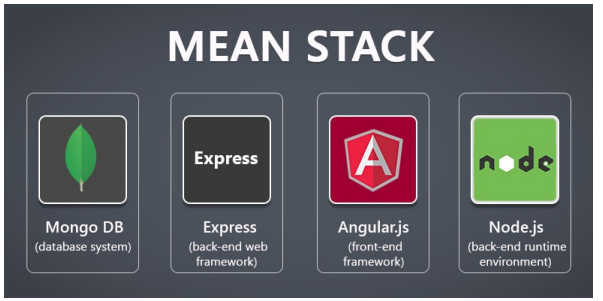


Exhaustivité des réponses

- Pourquoi Debian et Talos répondent-ils à si peu de vulnérabilités ?
  - Certaines vulnérabilités ne sont pas pertinentes pour une distribution Linux
  - Certaines vulnérabilités ne sont pas pertinentes pour un IDS réseau
- Debian et Talos sont-ils « exhaustifs » dans leur processus de réponse aux vulnérabilités ?

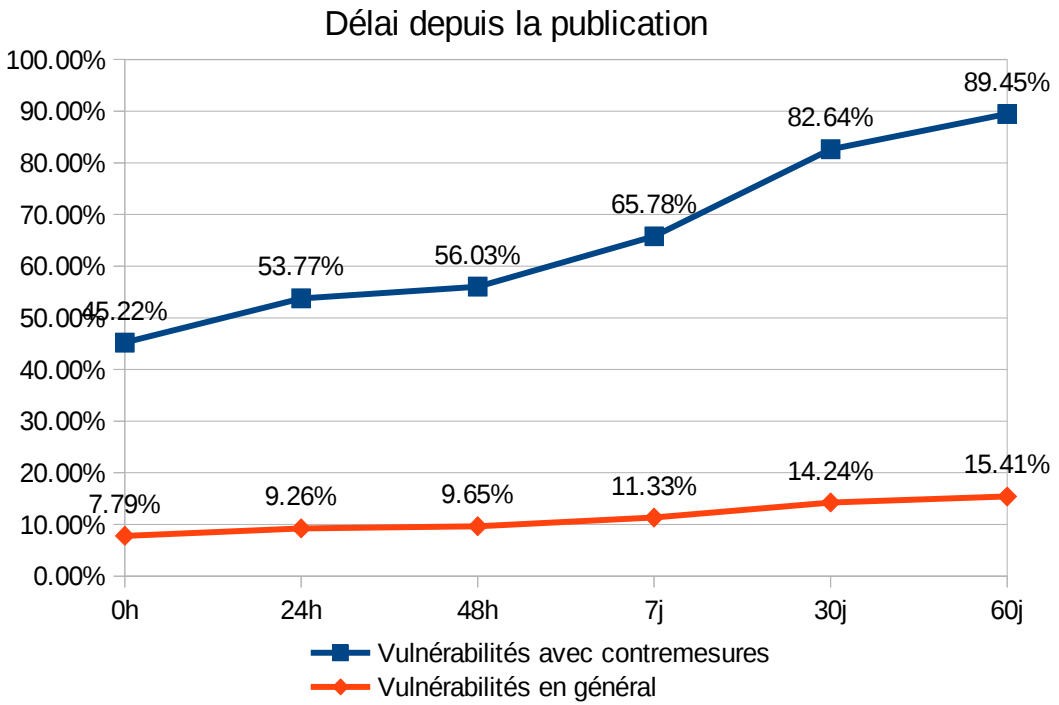
Étude complémentaire

- Exhaustivité des réponses : une question non triviale
- Analyse manuelle des vulnérabilités critiques de trois piles logicielles cloud typiques
  - Aucune vulnérabilité laissée sans réponse dans cet échantillon



Résultats avec hypothèse exhaustive

- Talos et Debian répondent à peu de vulnérabilités
  - Seulement 17.23 % des vulnérabilités reçoivent une contre-mesure
  - Mais cela inclut **probablement** la majorité des vulnérabilités « importantes » pour un client cloud
- La majorité des contre-mesures sont publiées rapidement, sans influence significative du score CVSS



Nos travaux

- Étude sur le cycle de vie des vulnérabilités et leurs contre-mesures

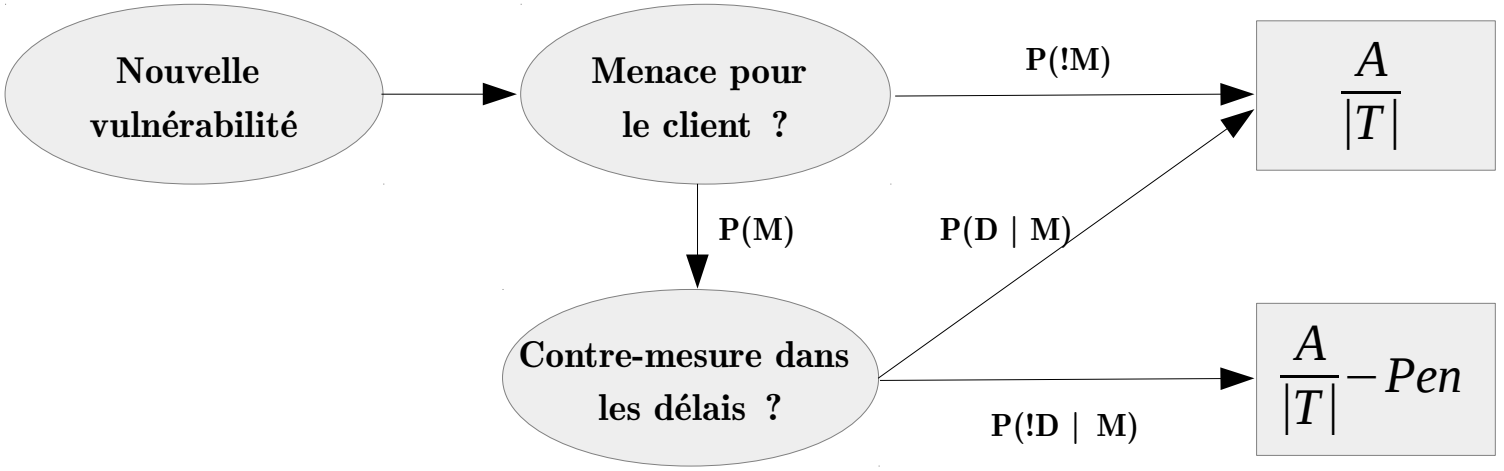
- **Modèle économique et contractuel formalisant l'engagement d'un fournisseur de cloud auprès de ses clients à prendre en compte la publication de vulnérabilités**

Conversation fictive

Fournisseur de cloud

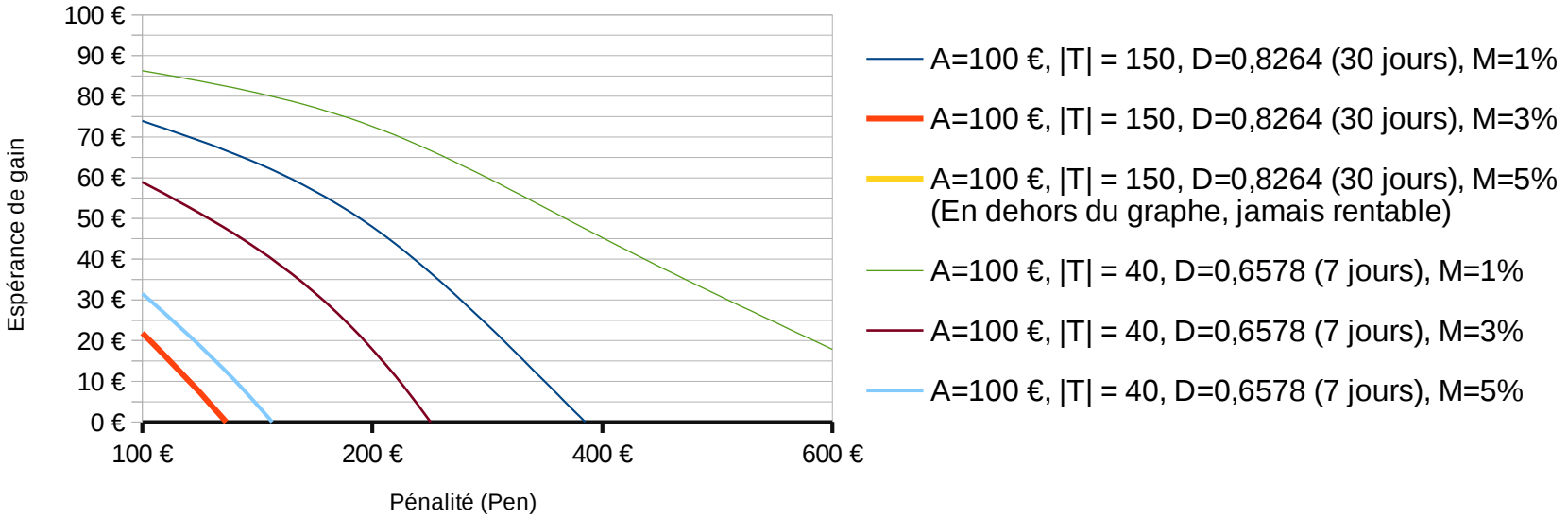
Client cloud

Modèle économique



- **A** : montant de l'abonnement payé par le client pour la période en cours
- **Pen** : montant agréé de la pénalité à rembourser par le fournisseur pour chaque vulnérabilité en dépassement de délai
- **T** : ensemble des nouvelles vulnérabilités publiées pendant la période en cours
- **M** : la nouvelle vulnérabilité étudiée constitue une menace pour le client
- **D** : le fournisseur propose une contre-mesure dans le respect du délai contractuel

Modèle économique



- Deux familles de scénarios
  - Délai contractuel de 30 jours pour toute vulnérabilité
  - Délai contractuel de 7 jours pour les vulnérabilités critiques
  - D et |T| sont paramétrés à partir des résultats de notre étude sur le cycle de vie des vulnérabilités

Modèle économique

- Espérance de gain du fournisseur de cloud positive dans de nombreuses situations
- Un fournisseur doit utiliser ses propres données pour étudier sa situation spécifique
  - Hétérogénéité (ou non) des piles logicielles des clients
- Décider si une vulnérabilité menace un client n'est pas trivial
  - Heuristique nécessaire
  - Risque d'un service déficient pour le client ou pas rentable pour le fournisseur de cloud

Conclusion

- Étude inédite sur le cycle de vie des vulnérabilités
  - Faible délai entre la publication d'une vulnérabilité et ses contre-mesures
- Nouveau modèle économique entre un fournisseur de cloud d'infrastructure et ses clients
  - Fourniture d'une réponse aux nouvelles vulnérabilités, dans un délai contractualisé
- Analyse de la rentabilité de ce modèle économique
  - Espérance de gain positive dans de nombreuses situations