Apprentissage supervisé et systèmes de détection : une approche de bout-en-bout impliquant les experts en sécurité

Anaël Beaugnon

anael.beaugnon@ssi.gouv.fr

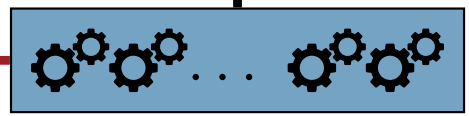
Thèse de doctorat encadrée par Francis Bach et Pierre Chifflier

25/06/2018

Sommaire

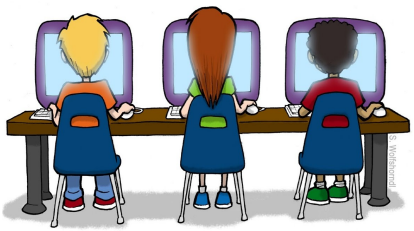
Système de détection

Communications



Alertes

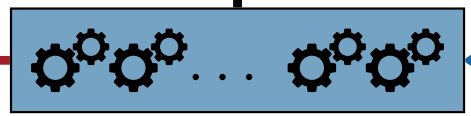
Système de détection



Opérateurs de sécurité

Système de détection

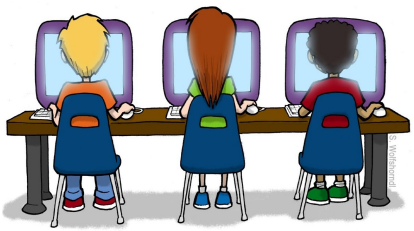
Communications



Système de détection

Alertes

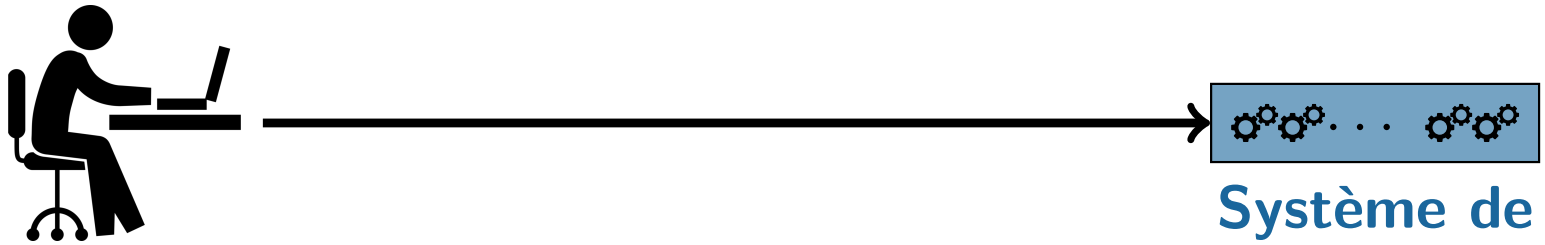
Cible de détection
Taxonomie des alertes



Opérateurs de sécurité

Administrateur de sécurité

Méthodes de détection et contraintes opérationnelles



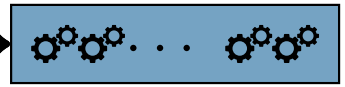
Administrateur de sécurité

Méthodes de détection

- Signatures
- Systèmes expert
- Détection d'anomalie
- Apprentissage supervisé

Méthodes de détection et contraintes opérationnelles

Contraintes opérationnelles



Système de détection

Administrateur de sécurité

Méthodes de détection

- Signatures
- Systèmes expert
- Détection d'anomalie
- Apprentissage supervisé

Contraintes opérationnelles

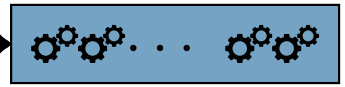
- Efficacité
- Transparence
- Robustesse

Rieck Computer security and machine learning: Worst enemies or best friends ?, 2011.

Sommer et al. Outside the closed world: on using machine learning for network intrusion detection, S&P'10.

Méthodes de détection et contraintes opérationnelles

Contraintes opérationnelles



Système de détection

Administrateur de sécurité

Méthodes de détection

- Signatures
- Systèmes expert
- Détection d'anomalie
- **Apprentissage supervisé**

Contraintes opérationnelles

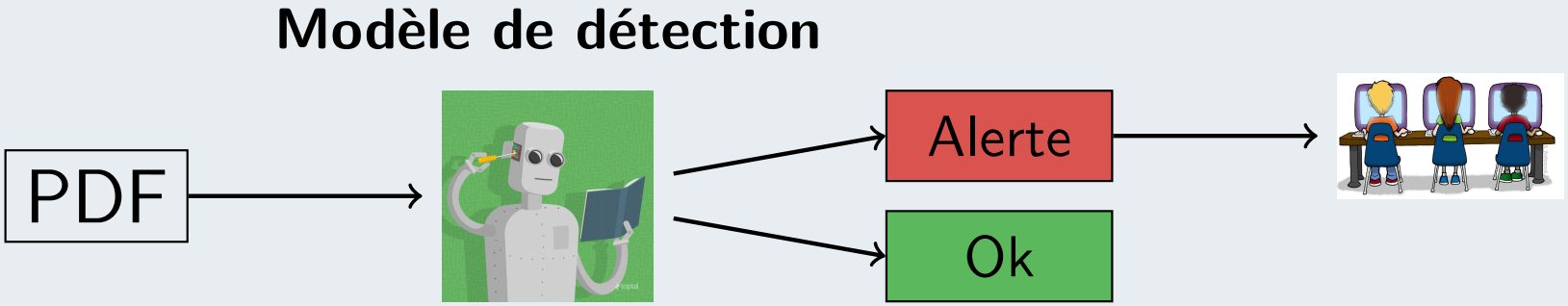
- Efficacité
- Transparence
- Robustesse

Rieck Computer security and machine learning: Worst enemies or best friends ?, 2011.

Sommer et al. Outside the closed world: on using machine learning for network intrusion detection, S&P'10.

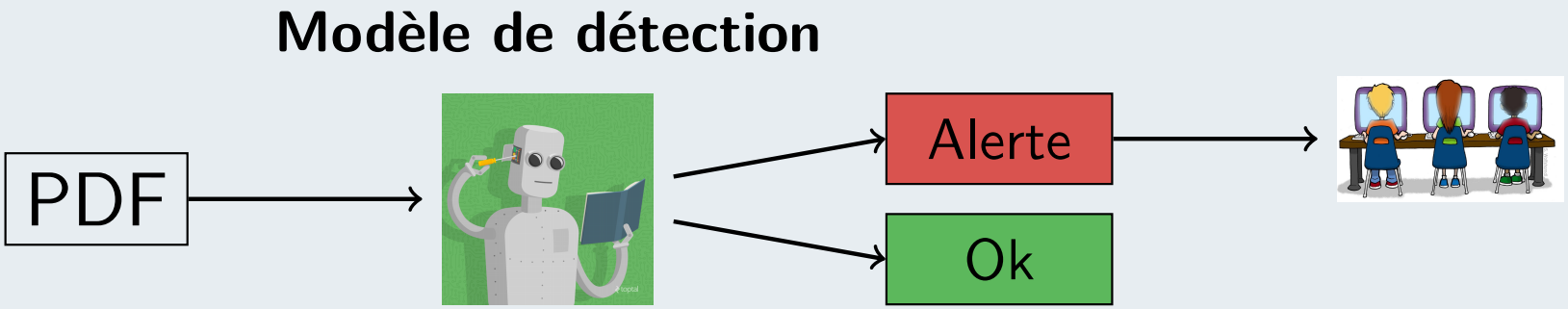
Modèle de détection supervisé

Un classifieur binaire

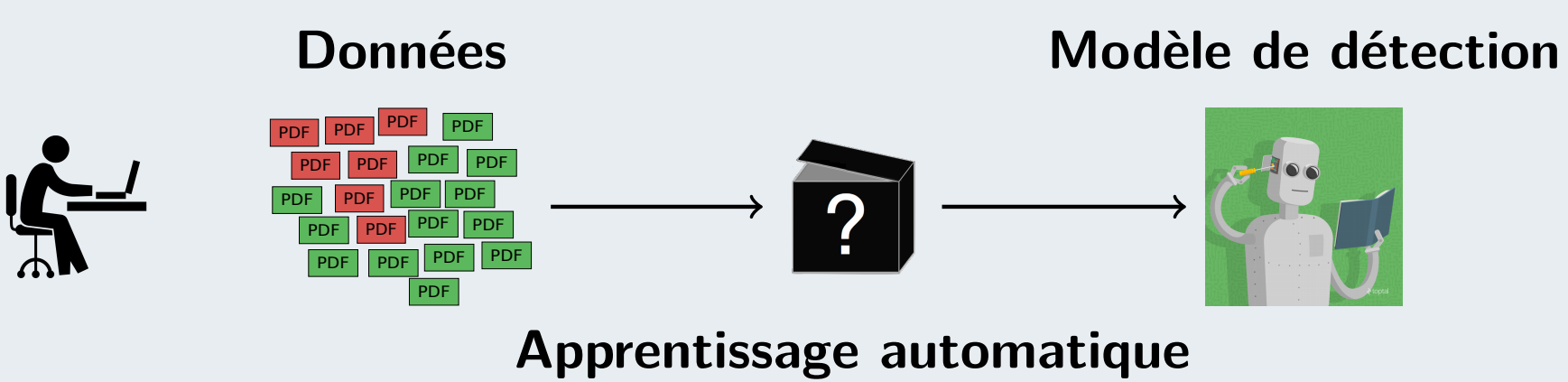


Modèle de détection supervisé

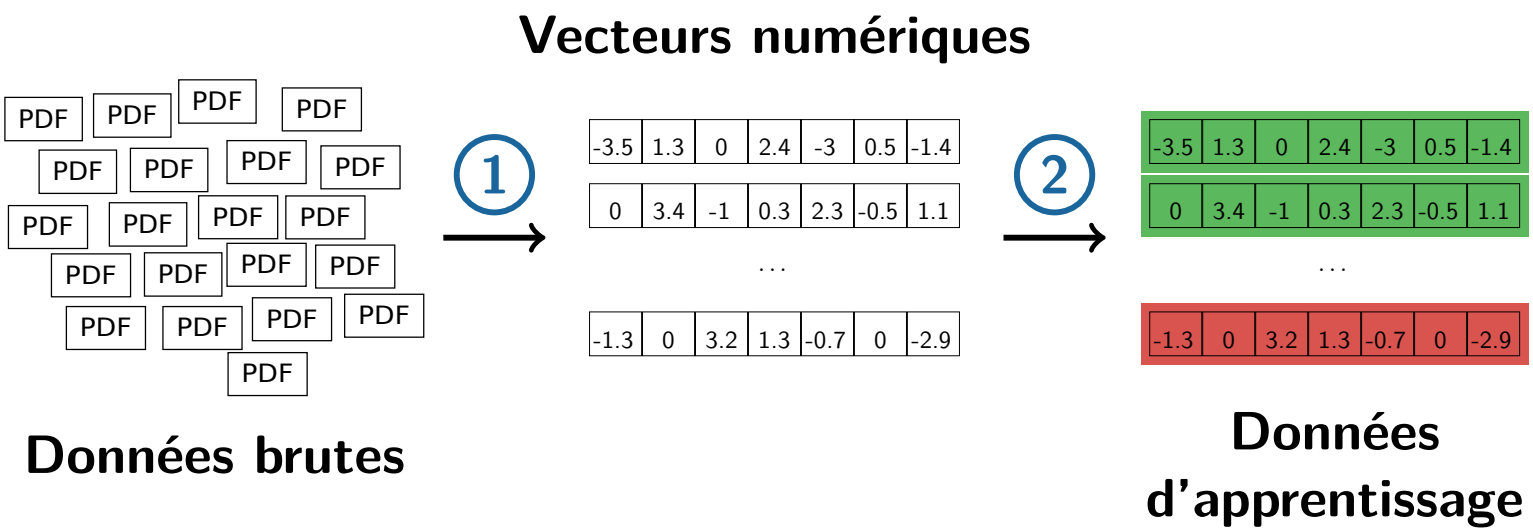
Un classifieur binaire



Apprentissage automatique

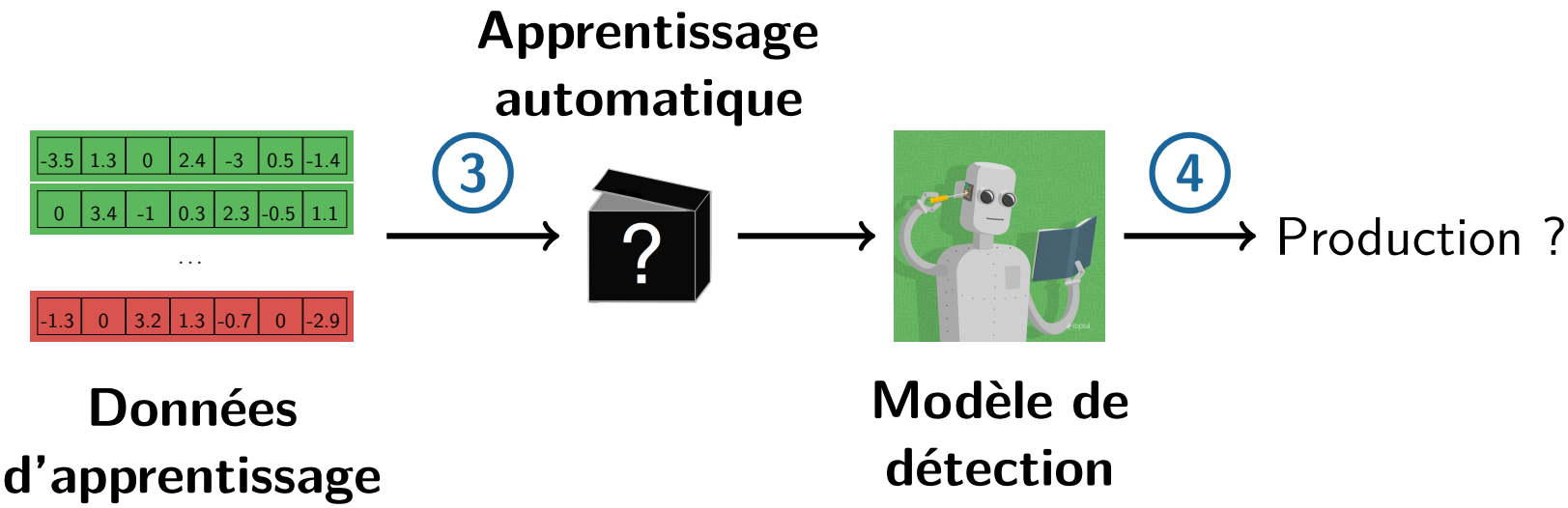


Données brutes → Données d'apprentissage



1. Extraction d'attributs
2. Annotation

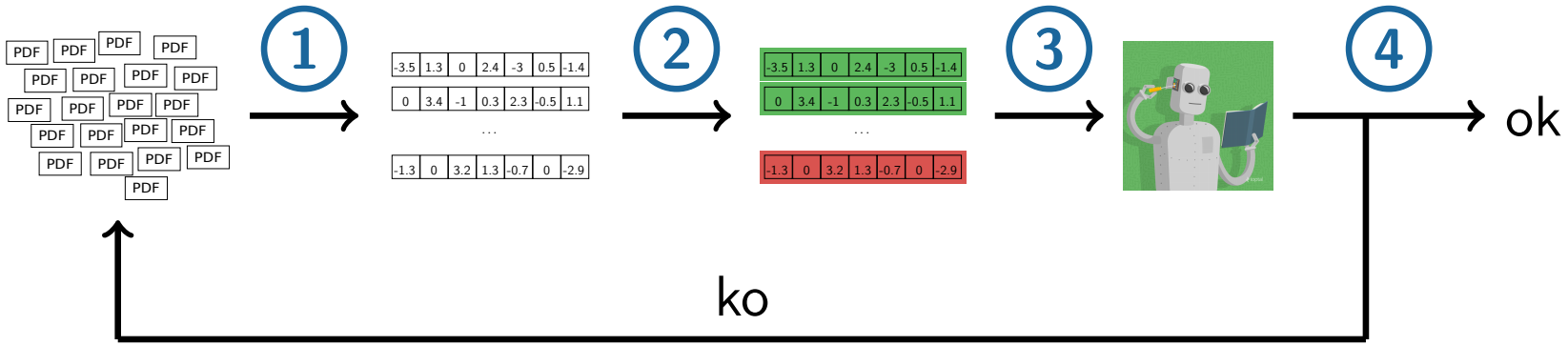
Apprentissage et validation du modèle



3 Classe de modèles ?

4 Validation

Chaîne de traitement de l'apprentissage supervisé



1. Extraction d'attributs
2. Annotation
3. Classe de modèles ?
4. Validation

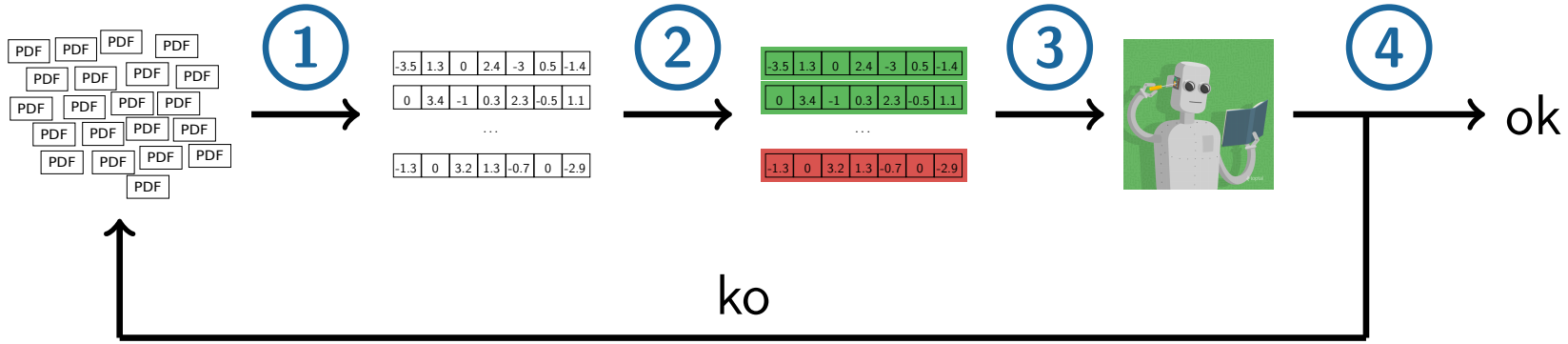
PDF Smutz et al., Malicious PDF detection using metadata and structural features, ACSAC'12.

Android Gascon et al., Structural detection of Android malware using embedded call graphs, AISEC'13.

Flash Overveldt et al., Flashdetect: Actionscript 3 malware detection, RAID'12.

Sommaire

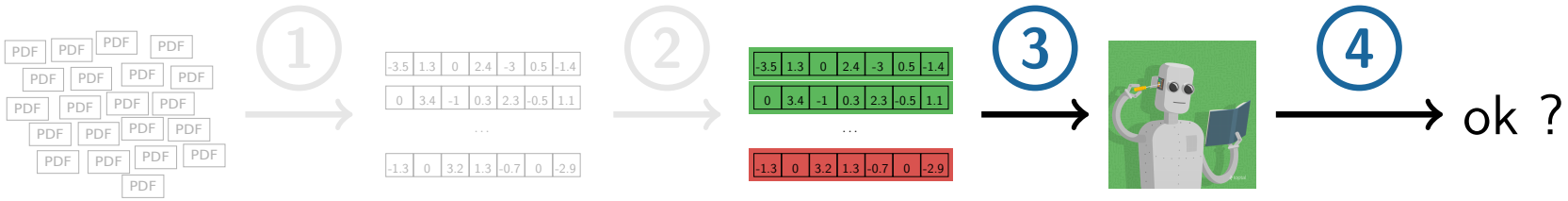
Une approche de bout-en-bout



1. Extraction d'attributs
2. Annotation
3. Classe de modèles ?
4. Validation

Wagstaff Machine learning that matters, ICML'12.

I- Mettre en place un modèle de détection supervisé



3 Classe de modèles ?

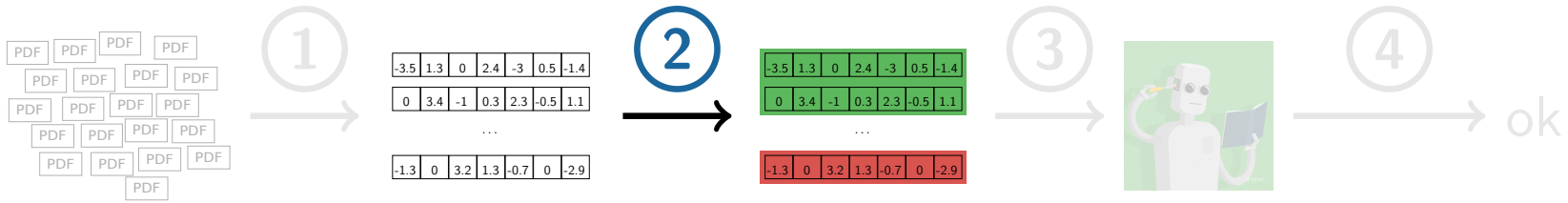
4 Validation

Contributions

- Méthodologie
- DIADEM : apprentissage et validation de modèles

SSTIC'17 **Le Machine Learning confronté aux contraintes opérationnelles des systèmes de détection**

II- Annoter un jeu de données avec un effort réduit



2 Annotation

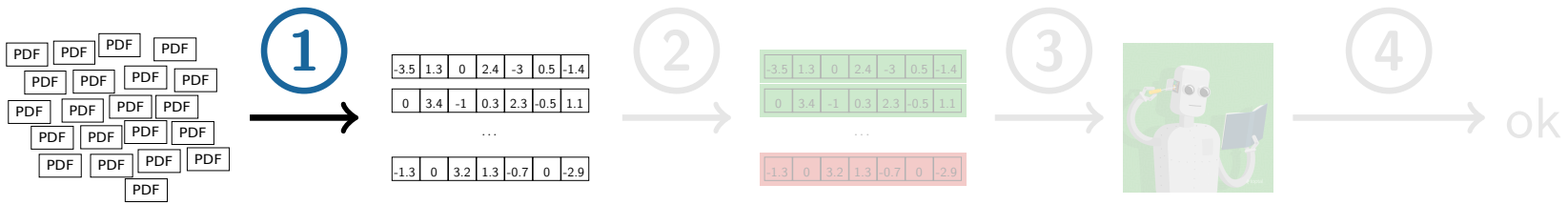
Contributions

- Stratégie d'apprentissage actif

  RAID'17 **ILAB: An Interactive Labelling Strategy for Intrusion Detection**
- Système d'annotations

  AICS'18, IDEA'18 **End-to-End Active Learning for Computer Security Experts**

III- Générer des attributs automatiquement



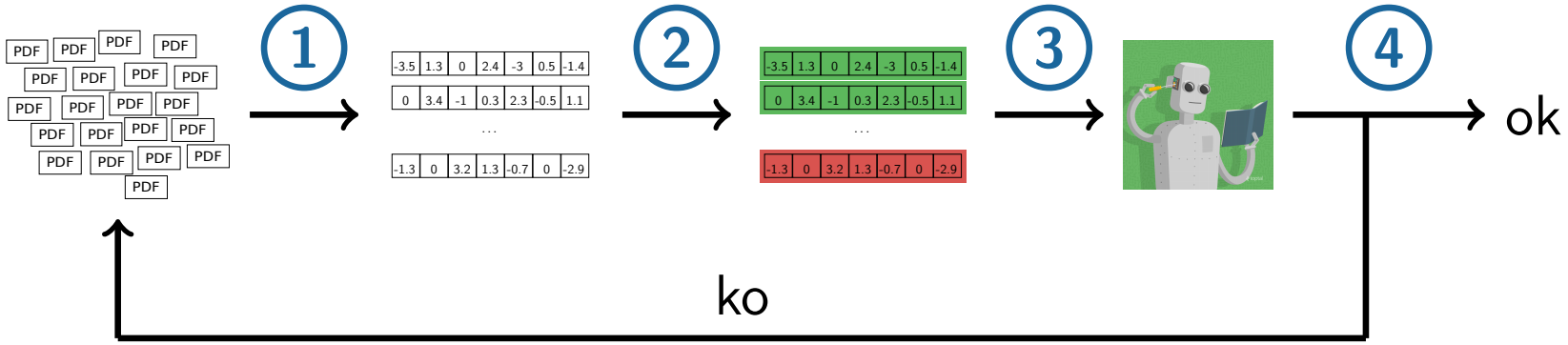
1 Extraction d'attributs

Contributions

- Comparaison de 3 méthodes (Khiops, Featuretools et Hidost)
- Pistes d'amélioration

Khiops Boulle, Towards automatic feature construction for supervised classification, ECML'14.
Featuretools Kanter et al., Deep feature synthesis: towards automating data science endeavors, DSAA' 15.
Hidost Šrndić et al., Hidost: a static machine learning based detector of malicious files, EURASIP'16.

Une approche de bout-en-bout



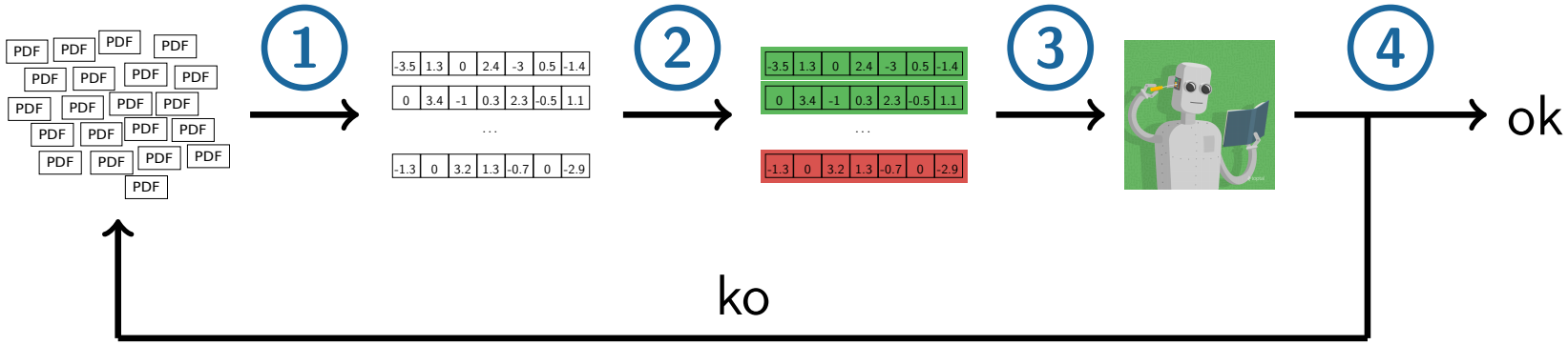
1. Apprentissage et validation ③
2. Annotation ②
3. Extraction d'attributs ①

③ et ④

②

①

Une approche de bout-en-bout



1. Apprentissage et validation (3) — 3 et 4
2. **Annotation** (2) — 2
3. Extraction d'attributs (1) — 1

Sommaire

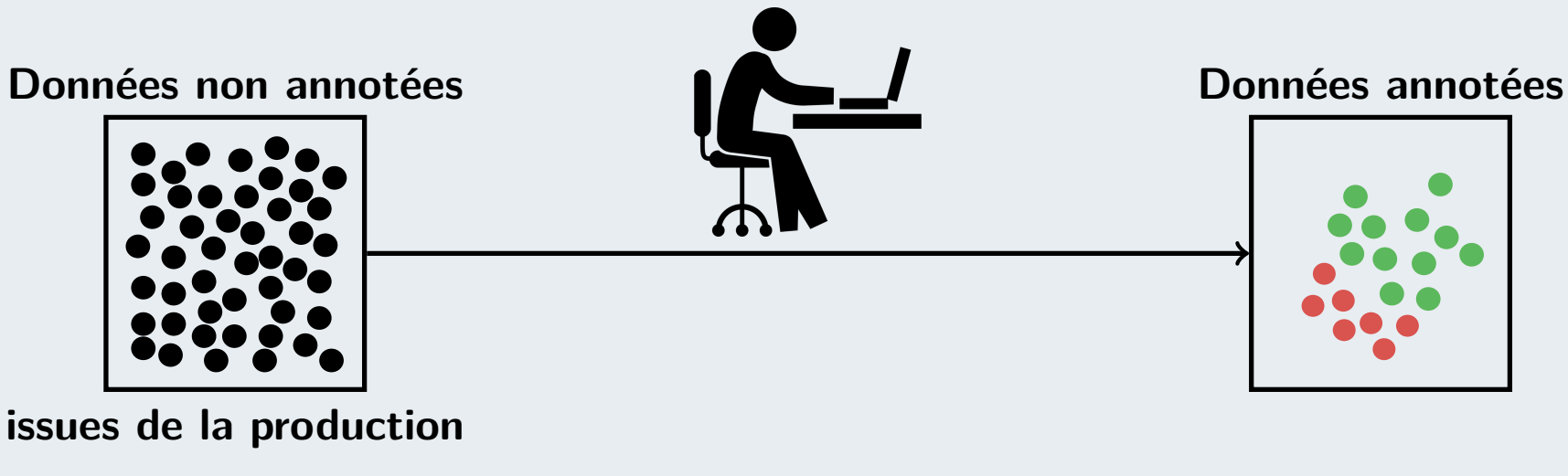
Manque de données annotées

- ✗ Jeux de données publics
- ✗ Crowd-sourcing

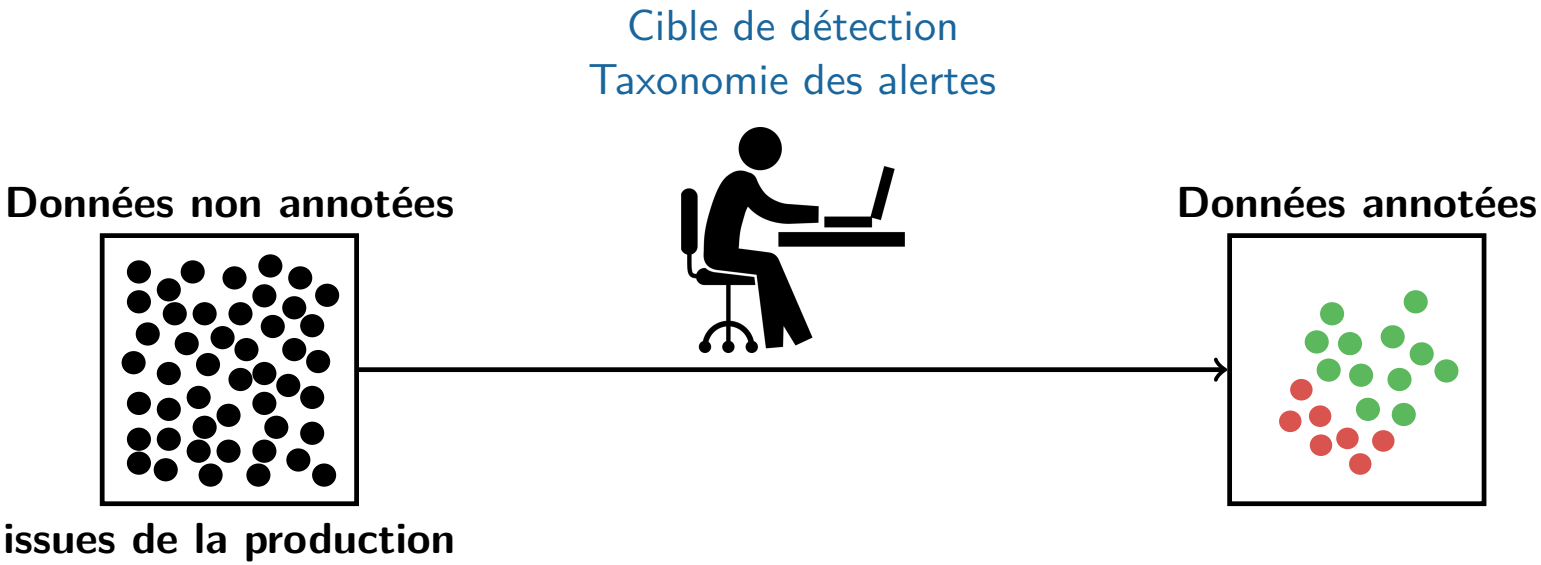
Manque de données annotées

- ✗ Jeux de données publics
- ✗ Crowd-sourcing

Solution : annotations in-situ



Annotations in-situ



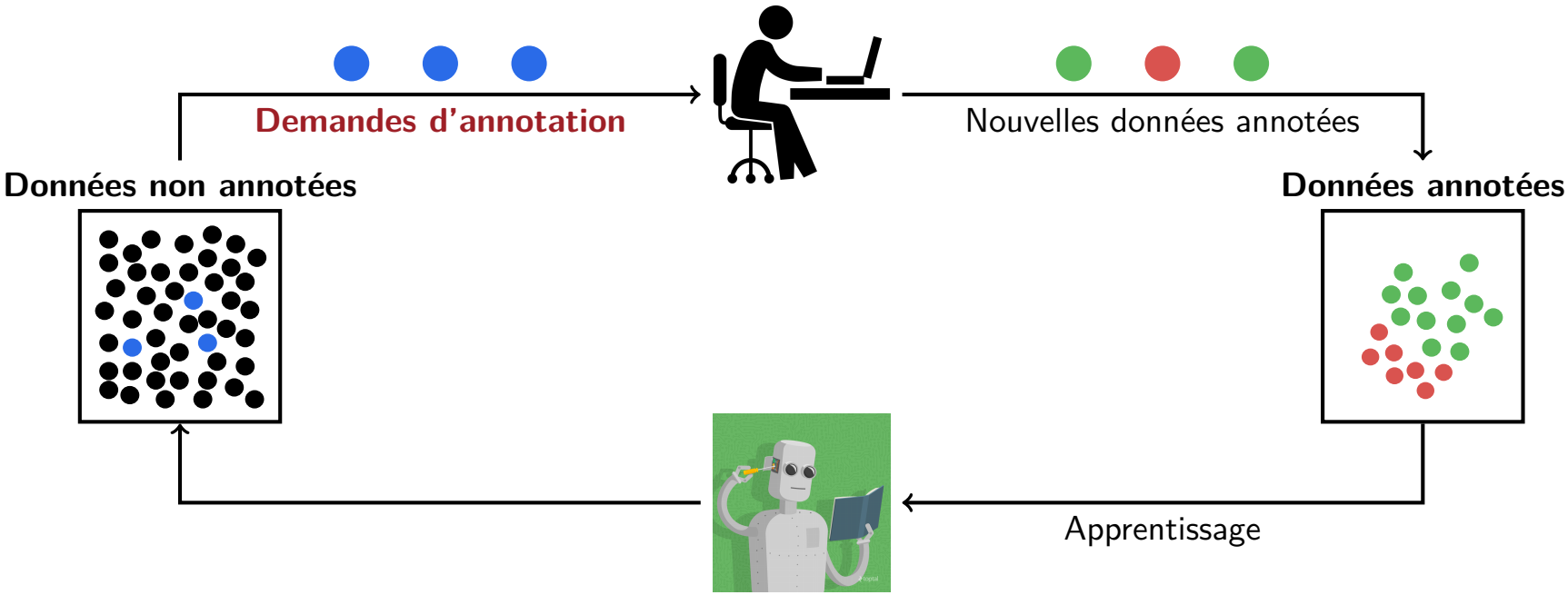
Annotation

label binaire
+
famille

Labels binaires $\longleftrightarrow$ Cible de détection

Familles malveillantes $\longleftrightarrow$ Taxonomie des alertes

Un processus itératif



Annotations in-situ

Objectifs

- Maximiser la performance du modèle de détection
- Minimiser l'effort humain
  - Nombre d'annotations
  - Temps global

Annotations in-situ

Objectifs

- Maximiser la performance du modèle de détection
- Minimiser l'effort humain
  - Nombre d'annotations
  - Temps global

Problématiques

1. Quelles instances doivent être annotées ?
   - ✗ Sélection aléatoire uniforme
2. Comment concevoir l'interface utilisateur ?

Annotations in-situ avec ILAB

Système d'apprentissage actif complet

Stratégie d'apprentissage actif

+

Système d'annotations

Stratégie d'apprentissage actif

Sélectionne les instances à annoter intelligemment.

RAID'17 **ILAB: An Interactive Labelling Strategy for Intrusion Detection**

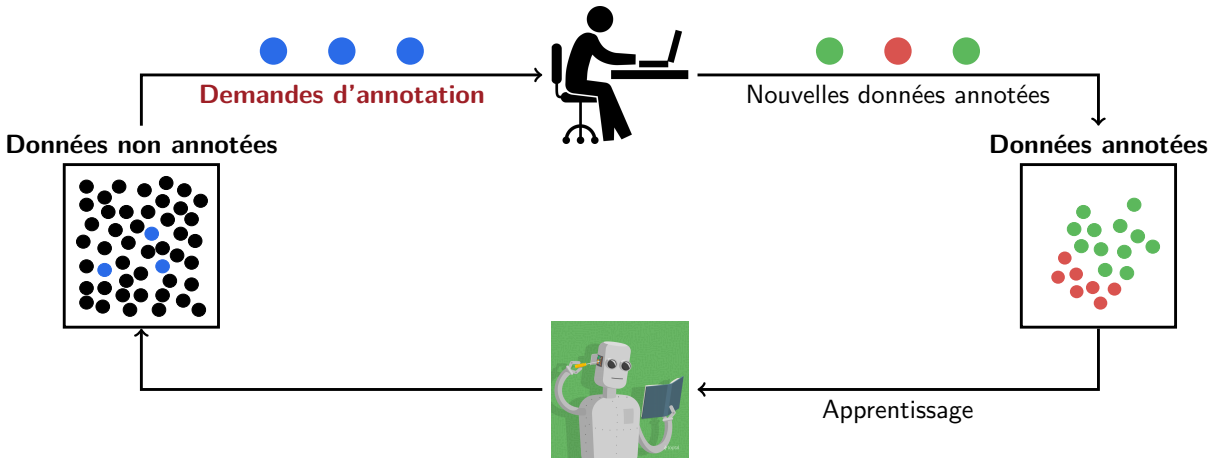
Système d'annotations

Adaptée aux besoins des experts en sécurité.

AICS'18, IDEA'18 **End-to-End Active Learning for Computer Security Experts**

Sommaire

Stratégie d'apprentissage actif



Quelles instances doivent être annotées ?

Objectifs

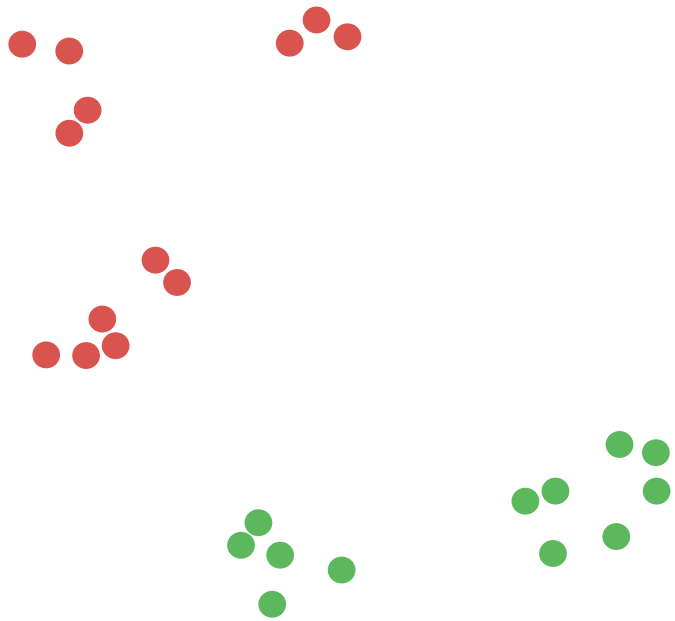
Pour un budget d'annotations B :

- Maximiser la performance de détection
- Minimiser le temps d'attente

Settles Active learning literature survey, 2010.

Uncertainty sampling

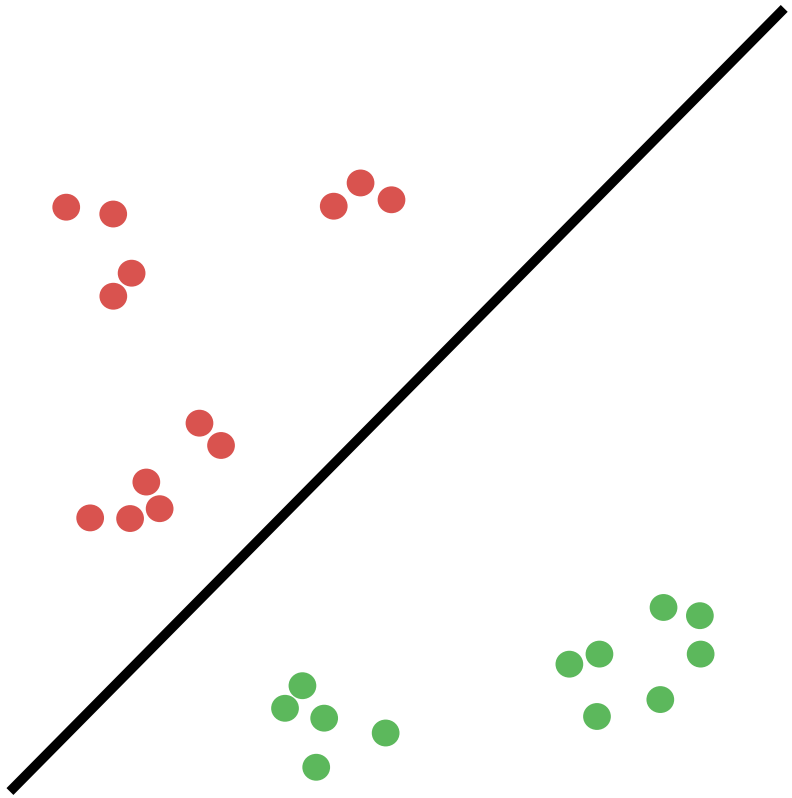
Une stratégie d'apprentissage actif



Lewis et al. A sequential algorithm for training text classifiers, 1994.

Uncertainty sampling

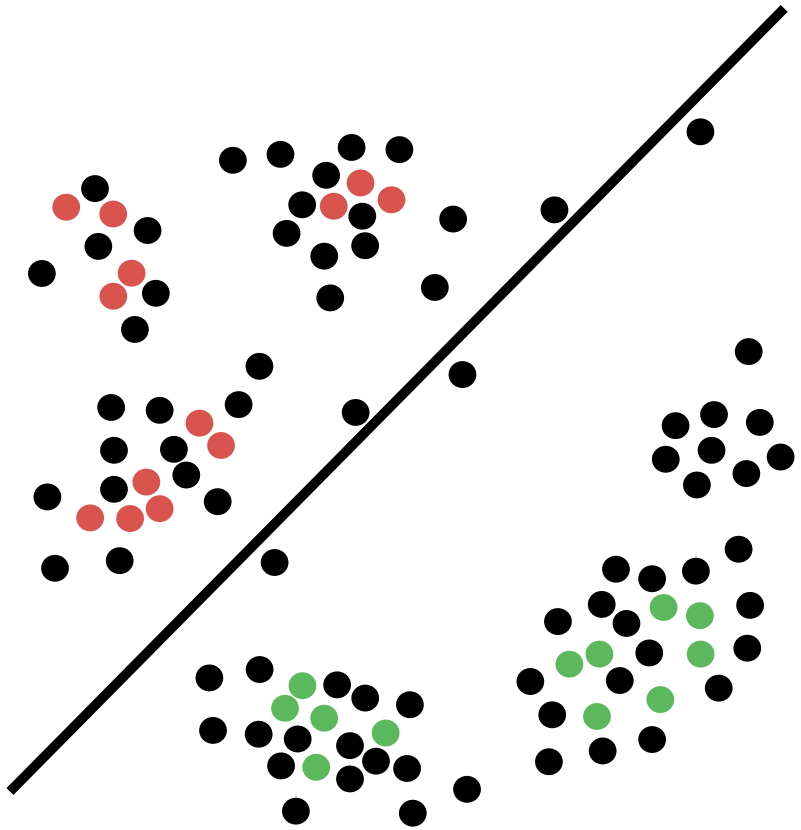
Une stratégie d'apprentissage actif



Lewis et al. A sequential algorithm for training text classifiers, 1994.

Uncertainty sampling

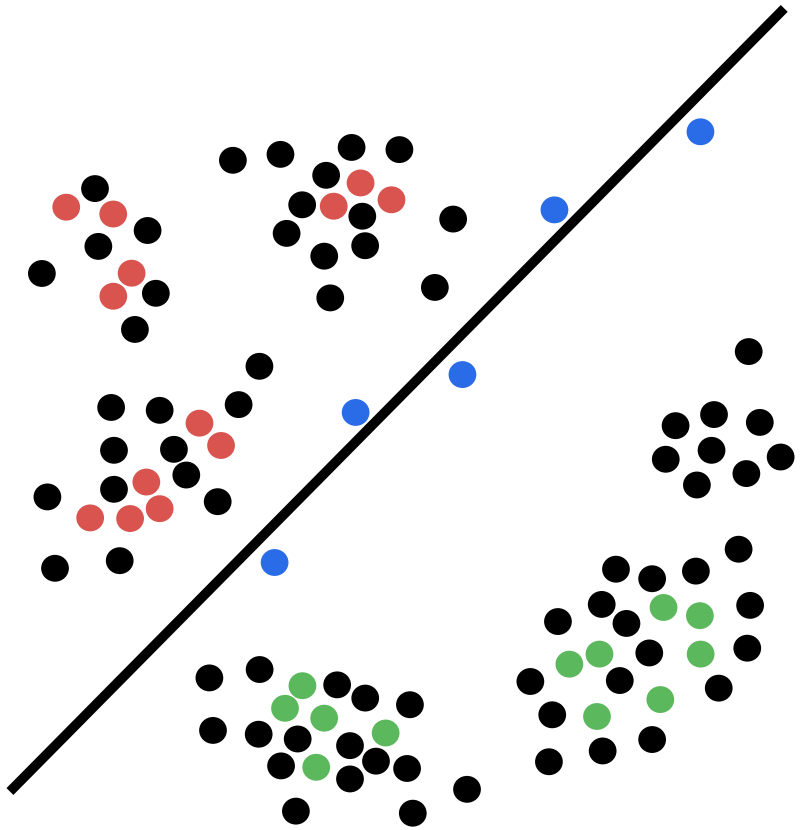
Une stratégie d'apprentissage actif



Lewis et al. A sequential algorithm for training text classifiers, 1994.

Uncertainty sampling

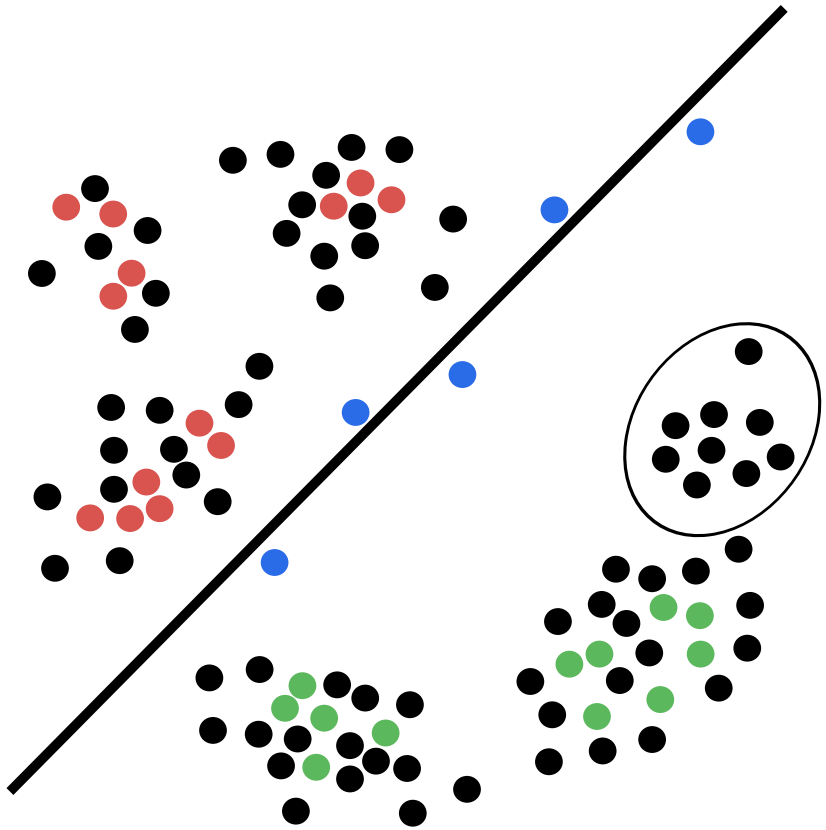
Une stratégie d'apprentissage actif



Lewis et al. A sequential algorithm for training text classifiers, 1994.

Uncertainty sampling

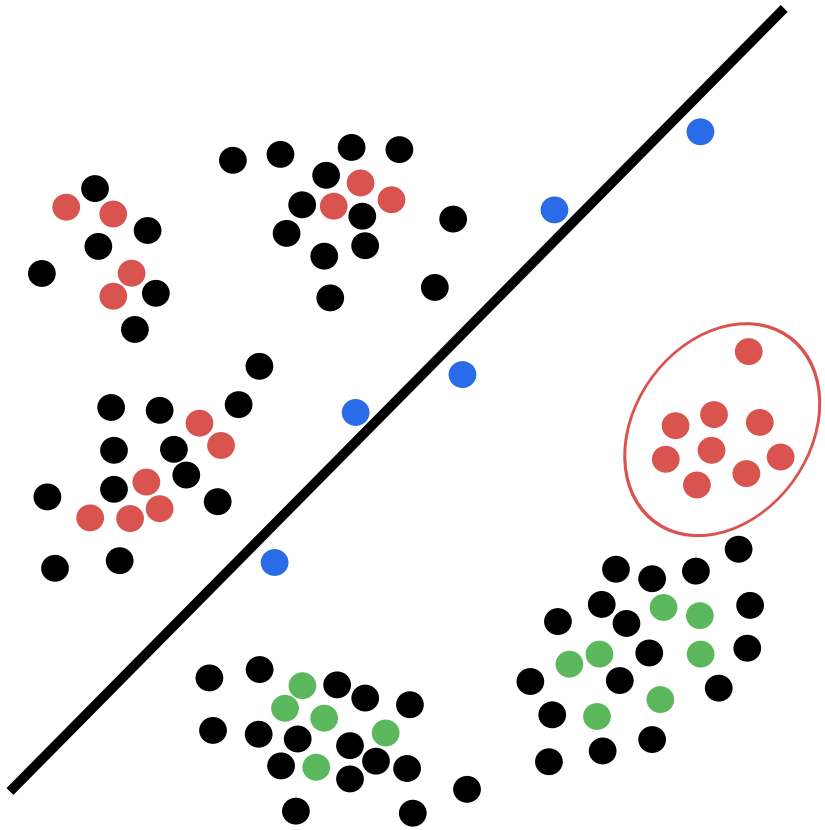
Une stratégie d'apprentissage actif



Lewis et al. A sequential algorithm for training text classifiers, 1994.

Uncertainty sampling

Une stratégie d'apprentissage actif



Lewis et al. A sequential algorithm for training text classifiers, 1994.

Schütz et al. Performance thresholding in practical text classification, CIKM'06.

Uncertainty sampling

Les biais d'échantillonnage détériorent les performances de détection.

	Uncertainty Sampling
Maximiser la performance de détection	✗
Minimiser le temps d'attente	✓

Uncertainty sampling

Les biais d'échantillonnage détériorent les performances de détection.

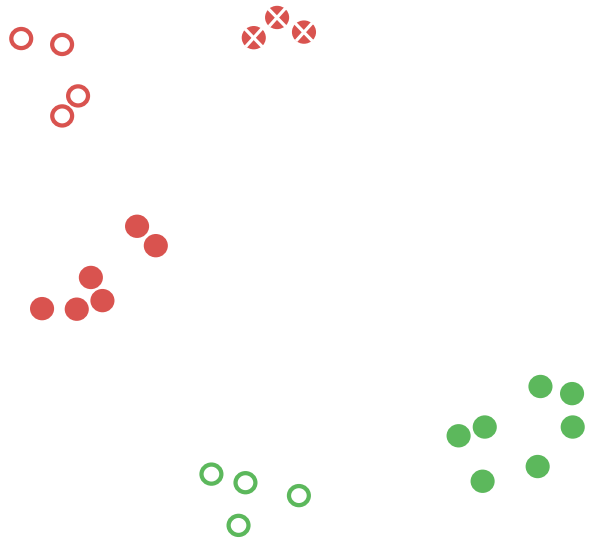
	Uncertainty Sampling
Maximiser la performance de détection	✗
Minimiser le temps d'attente	✓

Comment éviter les biais d'échantillonnage sans augmenter le temps d'attente ?

ILAB : stratégie d'apprentissage actif

Éviter les biais d'échantillonnage

Annotation : label binaire + famille



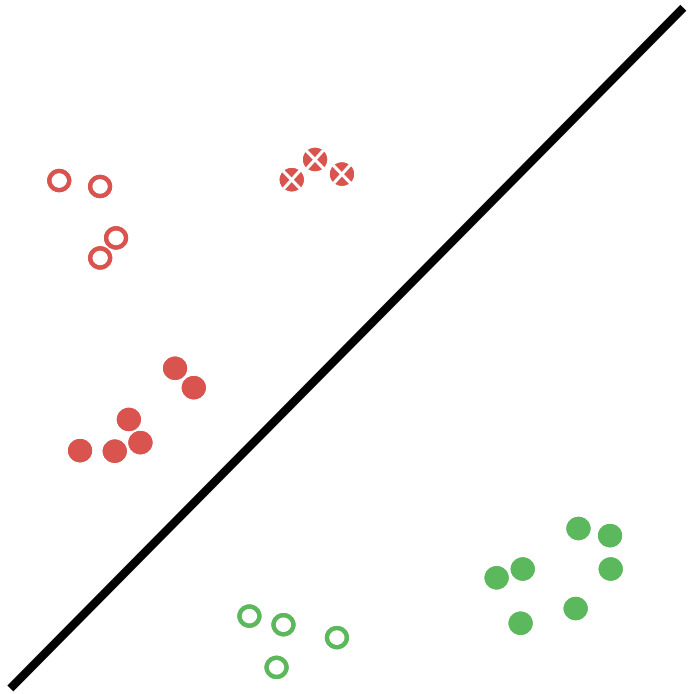
ILAB : stratégie d'apprentissage actif

Éviter les biais d'échantillonnage

Annotation : label binaire + famille

1. Régression logistique binaire

$$P(y = 1 \mid x) = \frac{1}{1+\exp\left(-\left(\mathbf{w}^T x + b\right)\right)}$$



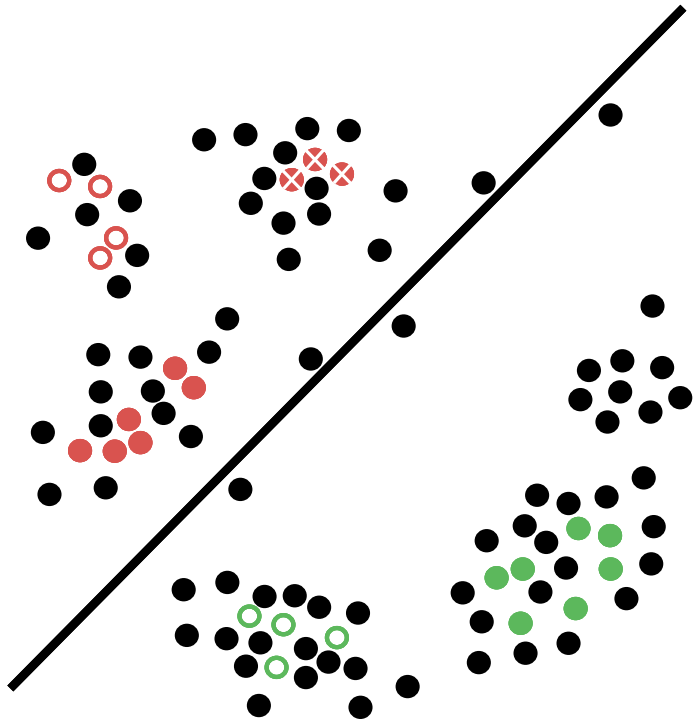
ILAB : stratégie d'apprentissage actif

Éviter les biais d'échantillonnage

Annotation : label binaire + famille

1. Régression logistique binaire

$$P(y = 1 \mid x) = \frac{1}{1+\exp\left(-\left(\mathbf{w}^T x + b\right)\right)}$$

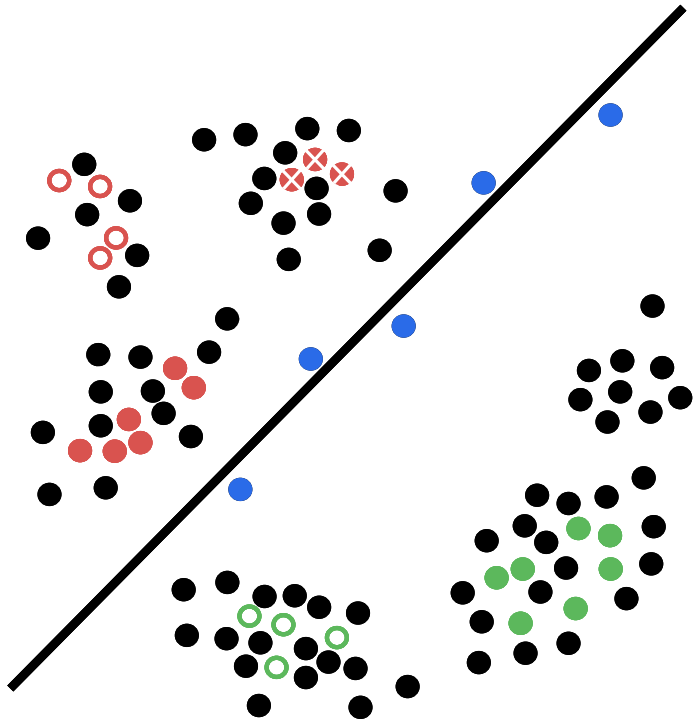


ILAB : stratégie d'apprentissage actif

Éviter les biais d'échantillonnage

Annotation : label binaire + famille

1. Régression logistique binaire
   $P(y = 1 \mid x) = \frac{1}{1+\exp\left(-\left(\mathbf{w}^T x + b\right)\right)}$
2. Uncertainty sampling

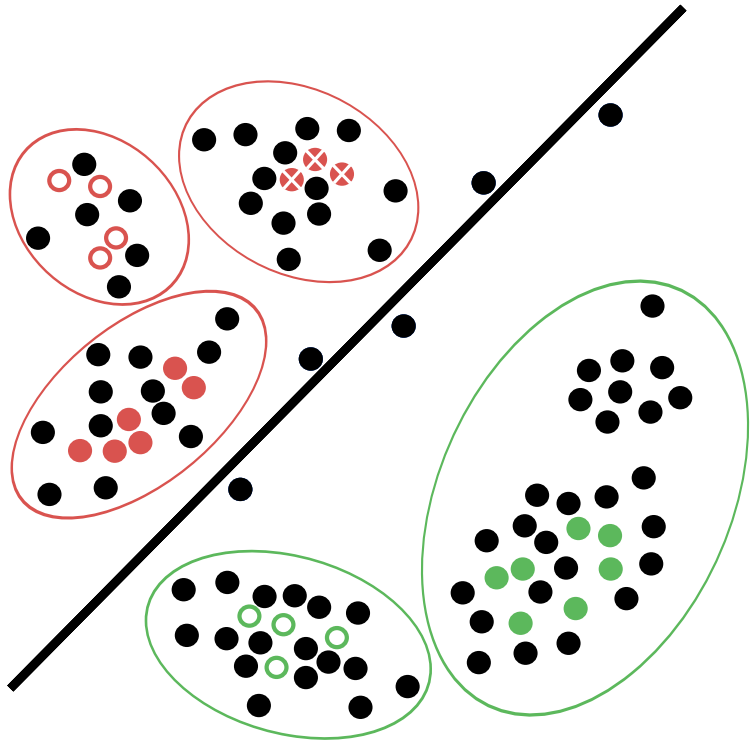


ILAB : stratégie d'apprentissage actif

Éviter les biais d'échantillonnage

Annotation : label binaire + famille

1. Régression logistique binaire
   $P(y = 1 \mid x) = \frac{1}{1+\exp\left(-\left(\mathbf{w}^T x + b\right)\right)}$
2. Uncertainty sampling
3. Détection de catégories rares



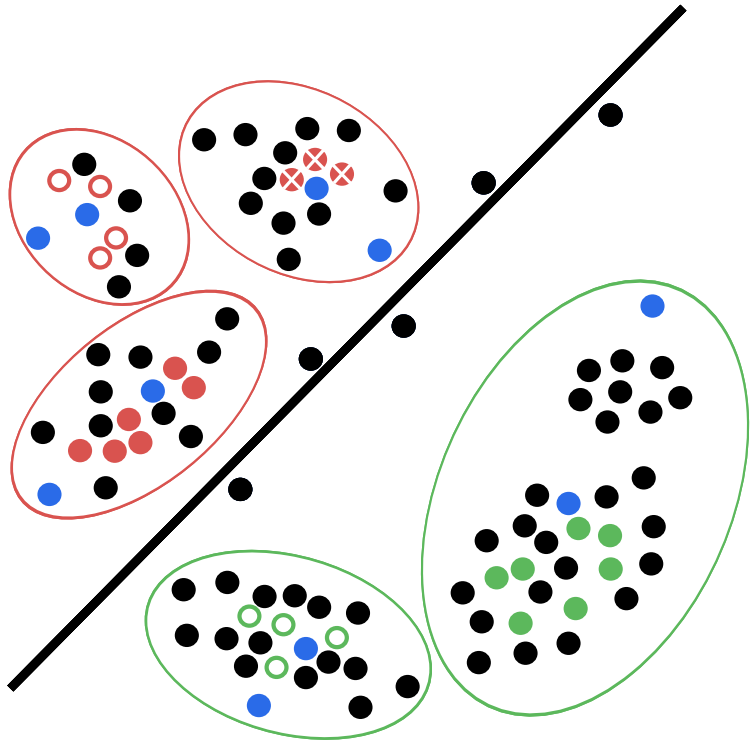
Clusters = Familles définies par l'utilisateur

ILAB : stratégie d'apprentissage actif

Éviter les biais d'échantillonnage

Annotation : label binaire + famille

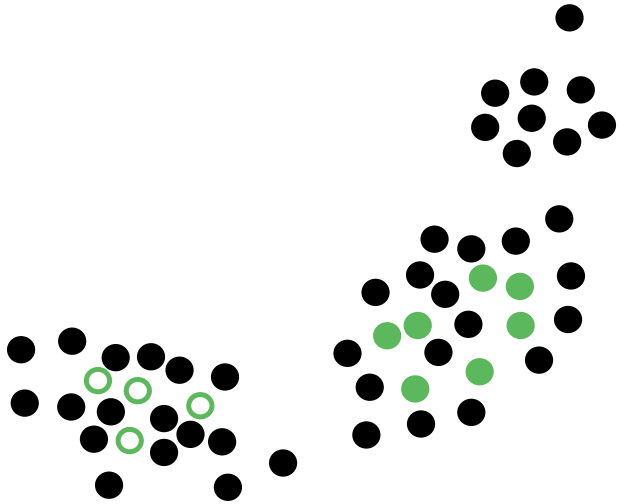
1. Régression logistique binaire
   $P(y = 1 \mid x) = \frac{1}{1+\exp\left(-\left(\mathbf{w}^T x + b\right)\right)}$
2. Uncertainty sampling
3. Détection de catégories rares



Clusters = Familles définies par l'utilisateur

Détection de catégories rares

Éviter les biais d'échantillonnage

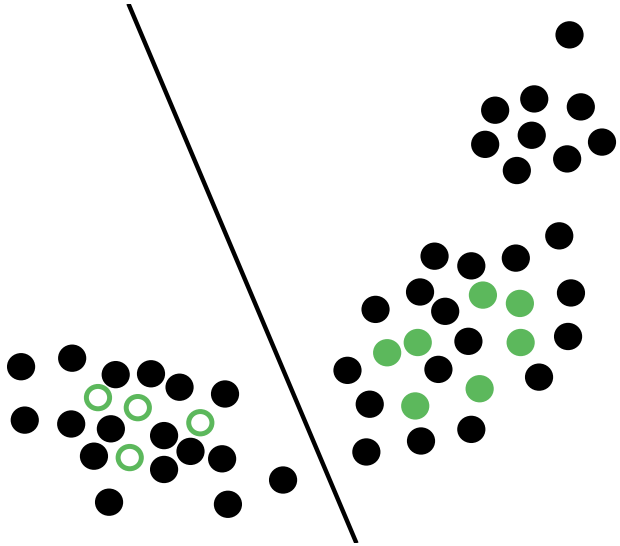


Pelleg et Moore Active learning for anomaly and rare category detection, NIPS'05.

Détection de catégories rares

Éviter les biais d'échantillonnage

1. Régression logistique multi-classes



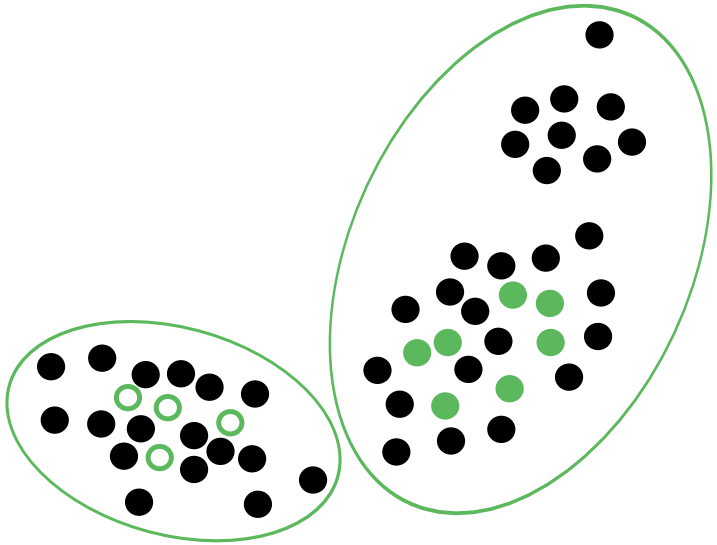
Pelleg et Moore Active learning for anomaly and rare category detection, NIPS'05.

Détection de catégories rares

Éviter les biais d'échantillonnage

1. Régression logistique multi-classes
2. Mélange de gaussiennes :

$$p_{\mathcal{N}(\mu_f,\Sigma_f)}(x) \propto \exp\left(-\frac{1}{2}\left\|\Sigma_f^{-\frac{1}{2}}(x-\mu_f)\right\|^2\right)$$



Pelleg et Moore Active learning for anomaly and rare category detection, NIPS'05.

Détection de catégories rares

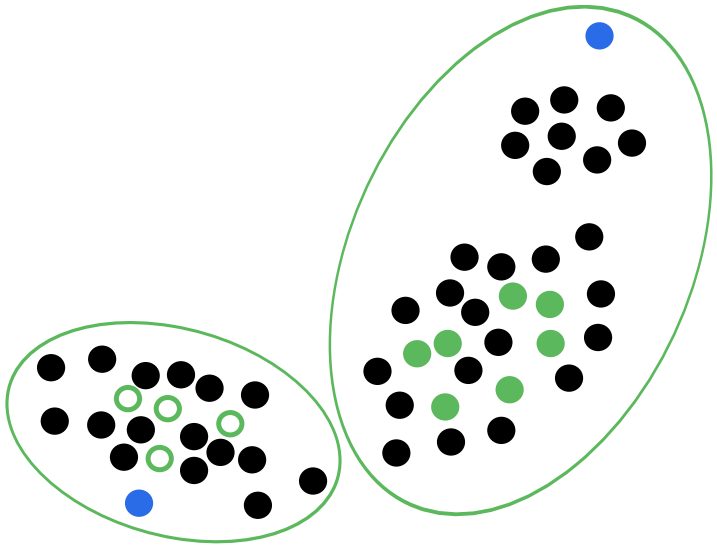
Éviter les biais d'échantillonnage

1. Régression logistique multi-classes
2. Mélange de gaussiennes :

$$p_{\mathcal{N}(\mu_f,\Sigma_f)}(x) \propto \exp\left(-\frac{1}{2}\left\|\Sigma_f^{-\frac{1}{2}}(x-\mu_f)\right\|^2\right)$$

3. Demandes d'annotations
   - **Détecter de nouvelles familles**

$$\arg\min_{x\in\mathcal{C}_f} p_{\mathcal{N}(\mu_f,\Sigma_f)}(x)$$



Pelleg et Moore Active learning for anomaly and rare category detection, NIPS'05.

Détection de catégories rares

Éviter les biais d'échantillonnage

1. Régression logistique multi-classes
2. Mélange de gaussiennes :

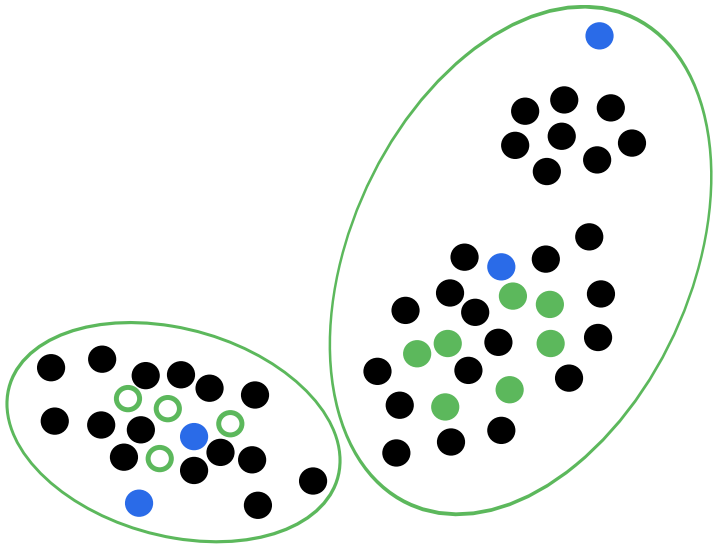
$$p_{\mathcal{N}(\mu_f,\Sigma_f)}(x) \propto \exp\left(-\frac{1}{2}\left\|\Sigma_f^{-\frac{1}{2}}(x-\mu_f)\right\|^2\right)$$

3. Demandes d'annotations
   - **Détecter de nouvelles familles**

$$\arg\min_{x\in\mathcal{C}_f} p_{\mathcal{N}(\mu_f,\Sigma_f)}(x)$$

   - **Instances représentatives**

$$\arg\max_{x\in\mathcal{C}_f} p_{\mathcal{N}(\mu_f,\Sigma_f)}(x)$$



Pelleg et Moore Active learning for anomaly and rare category detection, NIPS'05.

Détection de catégories rares

Éviter les biais d'échantillonnage

1. Régression logistique multi-classes
2. Mélange de gaussiennes :

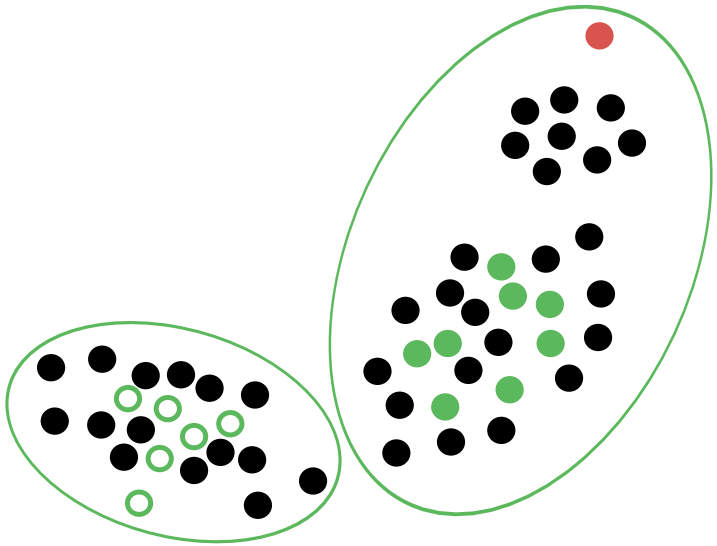
$$p_{\mathcal{N}(\mu_f,\Sigma_f)}(x) \propto \exp\left(-\frac{1}{2}\left\|\Sigma_f^{-\frac{1}{2}}(x-\mu_f)\right\|^2\right)$$

3. Demandes d'annotations
   - **Détecter de nouvelles familles**

$$\arg\min_{x\in\mathcal{C}_f} p_{\mathcal{N}(\mu_f,\Sigma_f)}(x)$$

   - **Instances représentatives**

$$\arg\max_{x\in\mathcal{C}_f} p_{\mathcal{N}(\mu_f,\Sigma_f)}(x)$$



Pelleg et Moore Active learning for anomaly and rare category detection, NIPS'05.

Détection de catégories rares

Éviter les biais d'échantillonnage

1. Régression logistique multi-classes
2. Mélange de gaussiennes :

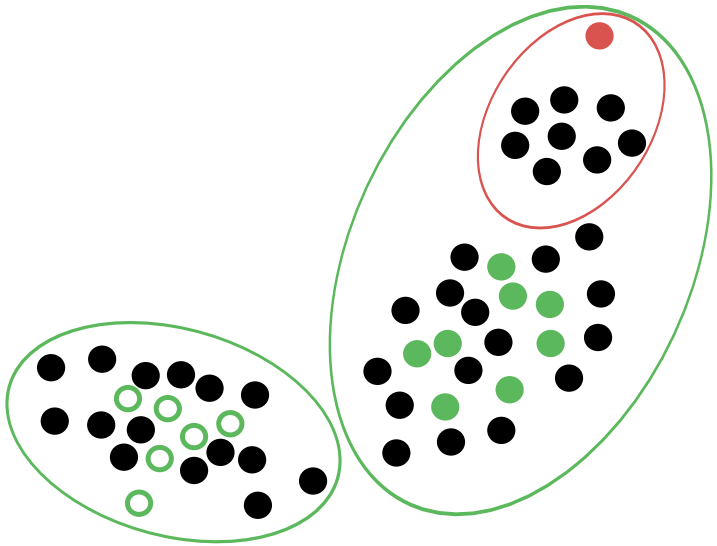
$$p_{\mathcal{N}(\mu_f,\Sigma_f)}(x) \propto \exp\left(-\frac{1}{2}\left\|\Sigma_f^{-\frac{1}{2}}(x-\mu_f)\right\|^2\right)$$

3. Demandes d'annotations
   - **Détecter de nouvelles familles**

$$\arg\min_{x\in\mathcal{C}_f} \; p_{\mathcal{N}(\mu_f,\Sigma_f)}(x)$$

   - **Instances représentatives**

$$\arg\max_{x\in\mathcal{C}_f} \; p_{\mathcal{N}(\mu_f,\Sigma_f)}(x)$$



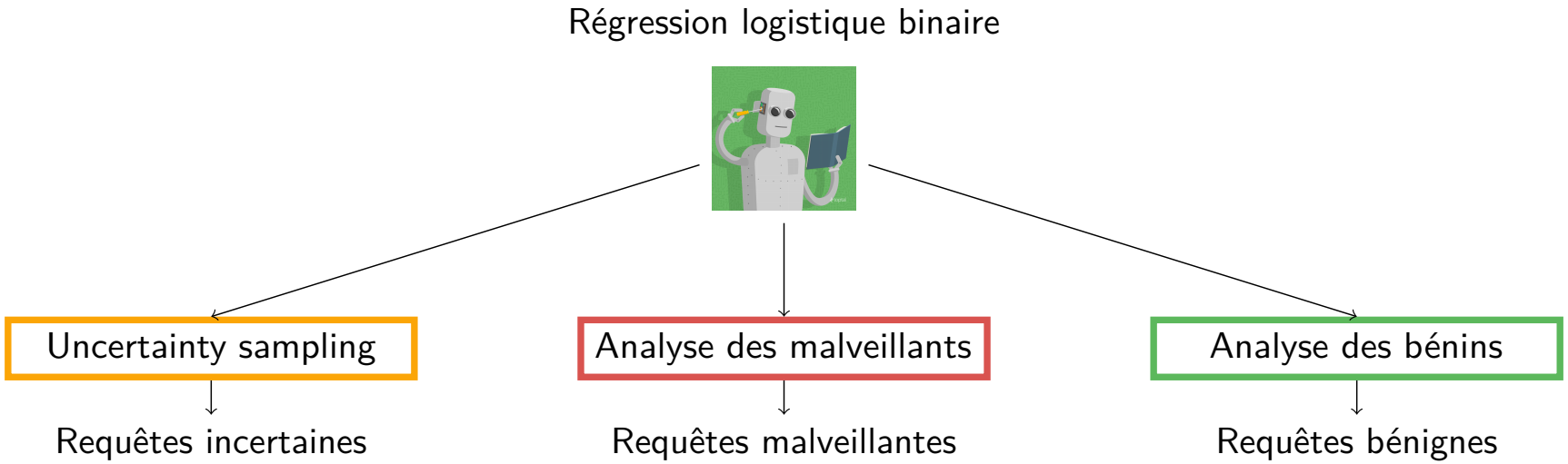
Pelleg et Moore Active learning for anomaly and rare category detection, NIPS'05.

ILAB : stratégie d'apprentissage actif

Réduire le temps d'attente

Diviser pour régner

- Réduction de la complexité
- Annotations pendant les calculs

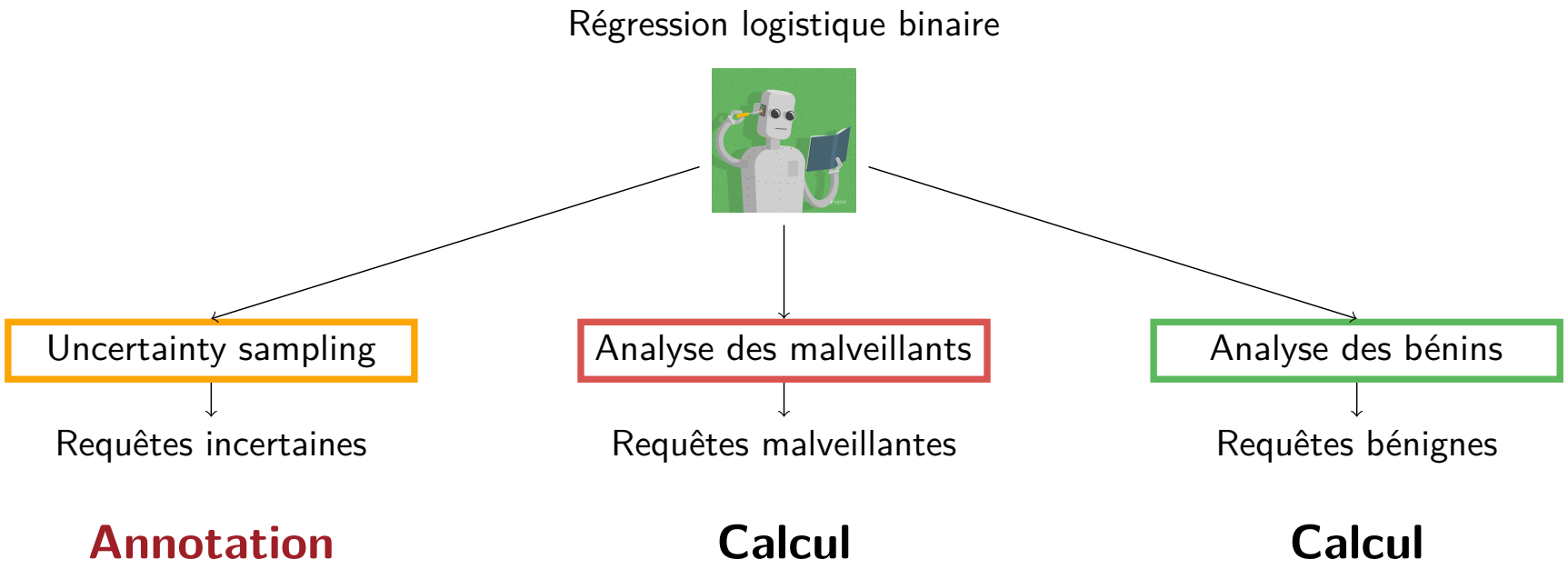


ILAB : stratégie d'apprentissage actif

Réduire le temps d'attente

Diviser pour régner

- Réduction de la complexité
- Annotations pendant les calculs



ILAB : stratégie d'apprentissage actif

Choix de conception

Éviter les biais d'échantillonnage

Détection de catégories rares

Réduire le temps d'attente

Diviser pour régner

Comparaison avec l'état de l'art

Simulations sur des jeux de données annotées

	#instances	#attributs
Contagio	$10,000$	113
NSL-KDD	$74,826$	122

Stratégies d'apprentissage actif

Uncertainty — Almgren et al., Using Active Learning in Intrusion Detection, CSFW 2004.

Görnitz et al. — Görnitz et al., Toward Supervised Anomaly Detection, JAIR 2013.

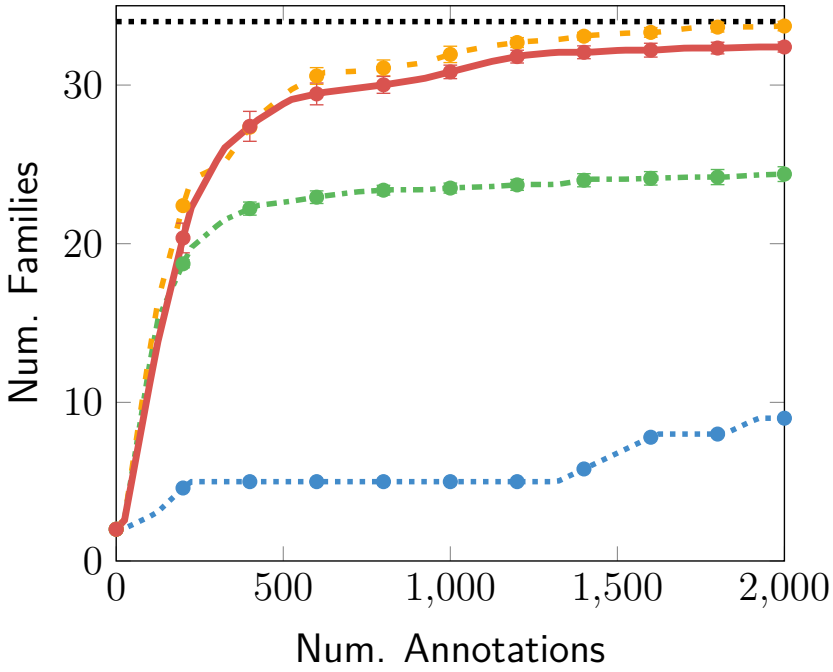
Aladin — Stokes et al., Aladin: Active Learning of Anomalies to Detect Intrusions, 2008.

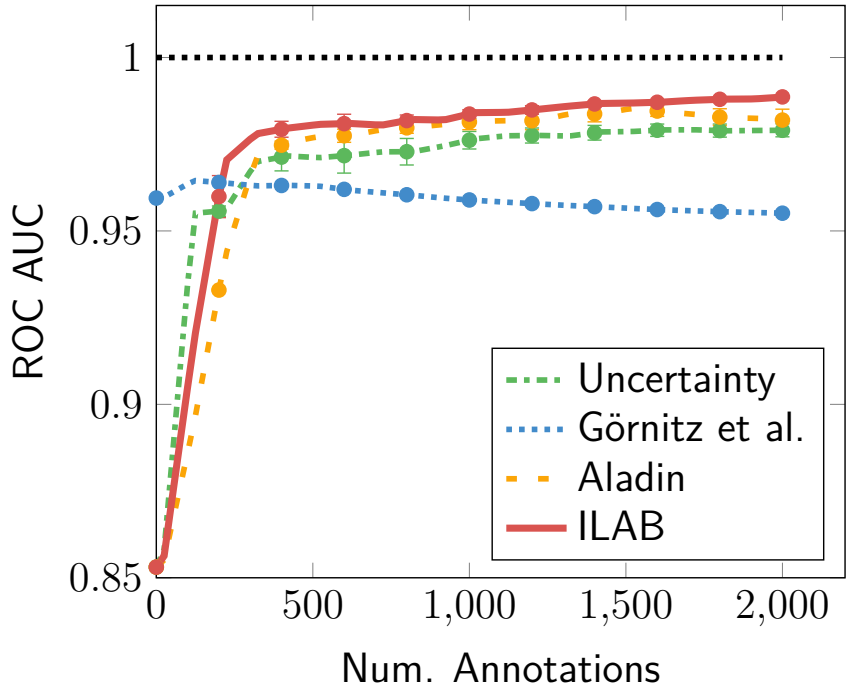
ILAB — **Beaugnon et al., ILAB: An Interactive Labelling Strategy for Intrusion Detection, RAID 2017.**

Comparaison avec l'état de l'art

Éviter les biais d'échantillonnage

ILAB et Aladin détectent bien les différentes familles.





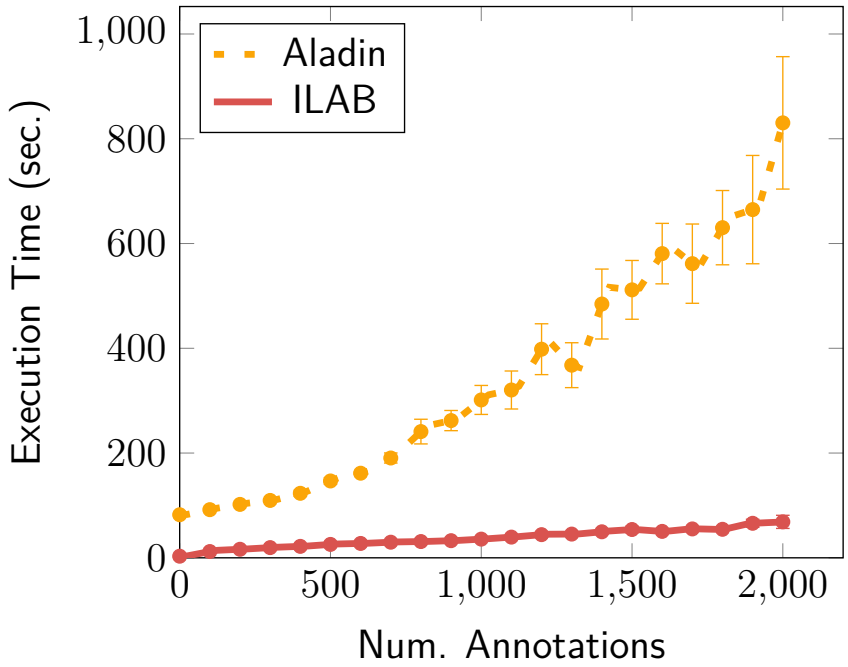
Uncertainty — Almgren et al., Using Active Learning in Intrusion Detection, CSFW 2004.

Görnitz et al. — Görnitz et al., Toward Supervised Anomaly Detection, JAIR 2013.

Aladin — Stokes et al., Aladin: Active Learning of Anomalies to Detect Intrusions, 2008.

ILAB — Beaugnon et al., ILAB: An Interactive Labelling Strategy for Intrusion Detection, RAID 2017.

Temps d'attente réduit grâce à ILAB



Aladin Stokes et al., Aladin: Active Learning of Anomalies to Detect Intrusions, 2008.

ILAB **Beaugnon et al., ILAB: An Interactive Labelling Strategy for Intrusion Detection, RAID 2017.**

Comparaison avec l'état de l'art

ILAB évite les biais d'échantillonnage sans augmenter le temps d'attente.

	Uncertainty	Görnitz et al.	Aladin	**ILAB**
Pas de biais	✗	✗	✓	✓
Rapide	✓	✗	✗	✓

https://github.com/ANSSI-FR/SecuML

Uncertainty Almgren et al., Using Active Learning in Intrusion Detection, CSFW 2004.

Görnitz et al. Görnitz et al., Toward Supervised Anomaly Detection, JAIR 2013.

Aladin Stokes et al., Aladin: Active Learning of Anomalies to Detect Intrusions, 2008.

ILAB **Beaugnon et al., ILAB: An Interactive Labelling Strategy for Intrusion Detection, RAID 2017.**

Comparaison avec l'état de l'art

ILAB évite les biais d'échantillonnage sans augmenter le temps d'attente.

	Uncertainty	Görnitz et al.	Aladin	**ILAB**
Pas de biais	✗	✗	✓	✓
Rapide	✓	✗	✗	✓

https://github.com/ANSSI-FR/SecuML

Uncertainty Almgren et al., Using Active Learning in Intrusion Detection, CSFW 2004.

Görnitz et al. Görnitz et al., Toward Supervised Anomaly Detection, JAIR 2013.

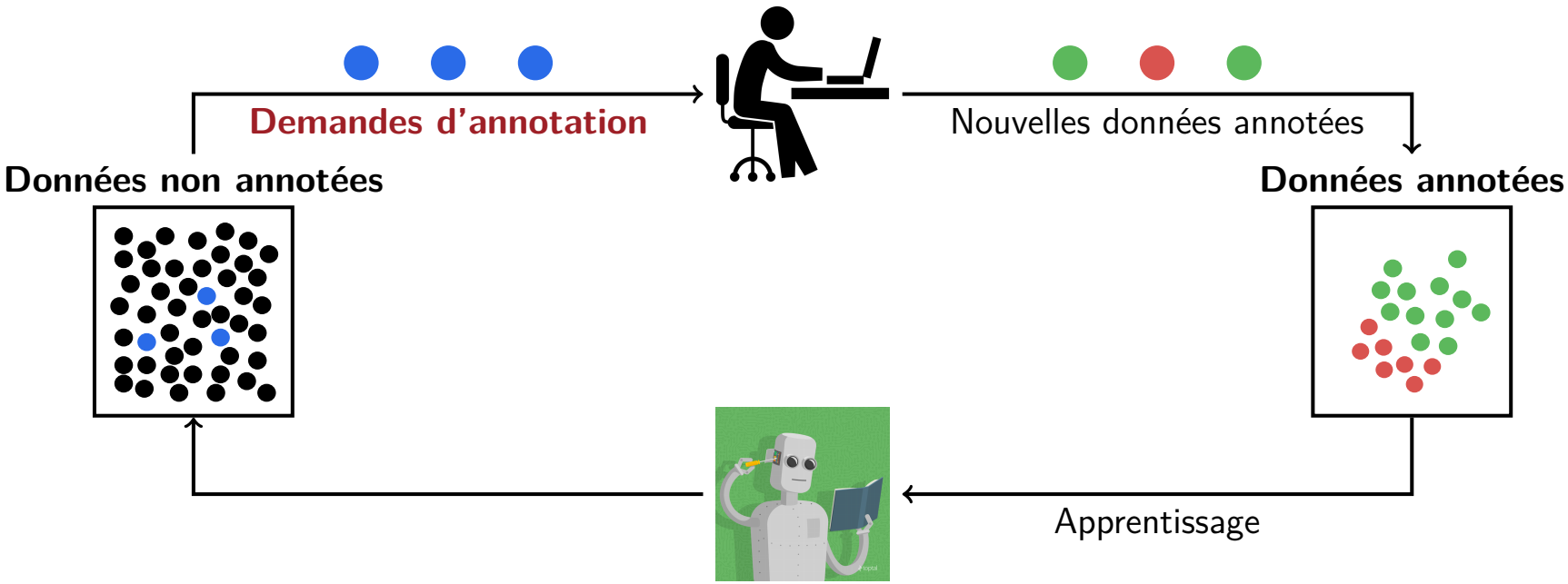
Aladin Stokes et al., Aladin: Active Learning of Anomalies to Detect Intrusions, 2008.

ILAB **Beaugnon et al., ILAB: An Interactive Labelling Strategy for Intrusion Detection, RAID 2017.**

Qu'en pensent les experts en sécurité ?

Sommaire

Ne pas oublier l'expert !



Comment concevoir l'interface utilisateur ?

Amershi et al. Power to the people: The role of humans in interactive machine learning, 2014.

Mac Aodha et al. Putting the scientist in the loop: accelerating scientific progress with interactive machine learning, ICPR'14.

Système d'annotations

Interface d'annotations

- Afficher les demandes d'annotations et collecter les réponses
- Afficher tout type de données
  - ex : PDF, documents Office, traces réseau.

Système d'annotations

Interface d'annotations

- Afficher les demandes d'annotations et collecter les réponses
- Afficher tout type de données
  - ex : PDF, documents Office, traces réseau.

Autres fonctionnalités

- Montrer à l'utilisateur que ces annotations sont utiles

Système d'annotations

Interface d'annotations

- Afficher les demandes d'annotations et collecter les réponses
- Afficher tout type de données
  - ex : PDF, documents Office, traces réseau.

Autres fonctionnalités

- Montrer à l'utilisateur que ces annotations sont utiles
- Aider l'utilisateur à rester cohérent au cours des itérations
  - Délimitation de la cible de détection
  - Définition de la taxonomie des alertes

Ne pas oublier l'expert !

	Simulations	GUI	Exp. utilisateur
Uncertainty	✓	✗	✗
Görnitz et al.	✓	✗	✗
Aladin	✓	∼	∼
Nissim et al.	✓	✗	✗
Moskovitch et al.	✓	✗	✗

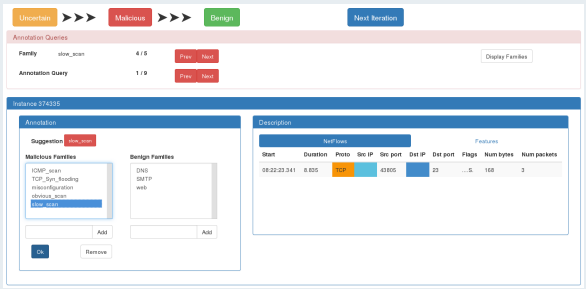
Aladin

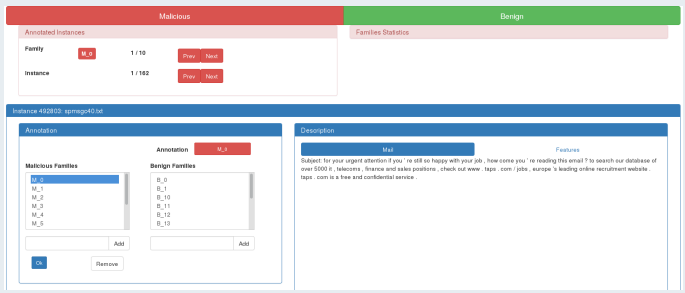
- Aucune information sur l'interface graphique
- 1000 annotations par jour sans aucun retour !

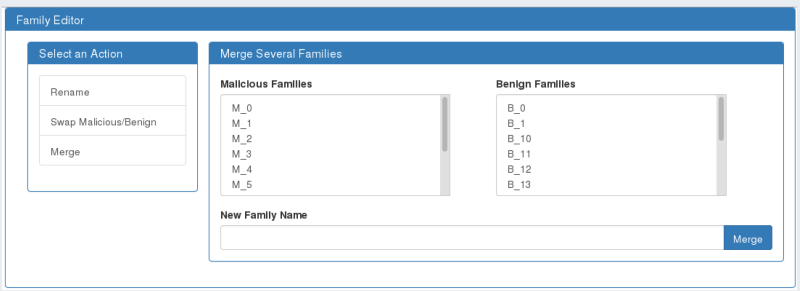
Uncertainty Almgren et al., Using Active Learning in Intrusion Detection, CSFW 2004
Görnitz et al. Toward Supervised Anomaly Detection, JAIR 2013
Aladin Stokes et al., Aladin: Active Learning of Anomalies to Detect Intrusions, 2008
Nissim et al. ALPD: Active learning framework for enhancing the detection of malicious PDF files, 2014.
Moskovitch et al. Malicious code detection using active learning, 2009.

ILAB : système d'annotations

Une interface graphique répondant aux besoins des experts en sécurité.







Quatre administrateurs de sécurité

Jeux de données

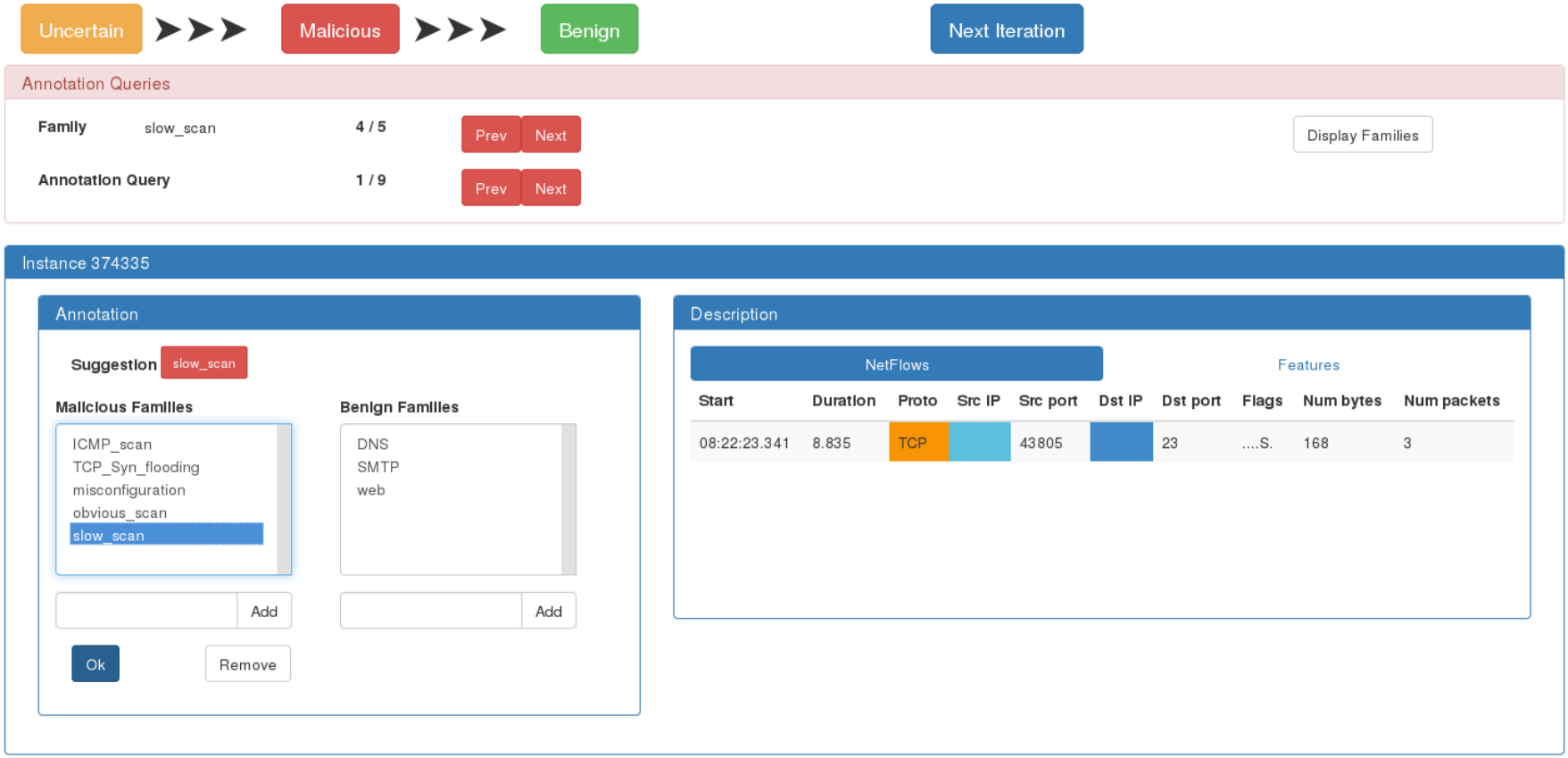
	Jour 1	Jour 2
Nb. flux	$1.2 \cdot 10^8$	$1.2 \cdot 10^8$
Nb. IP	$463,913$	$507,258$
Nb. attributs	134	134

Annotations initiales

- Données anormales
  Scans évidents
- Données normales
  Sélection uniforme

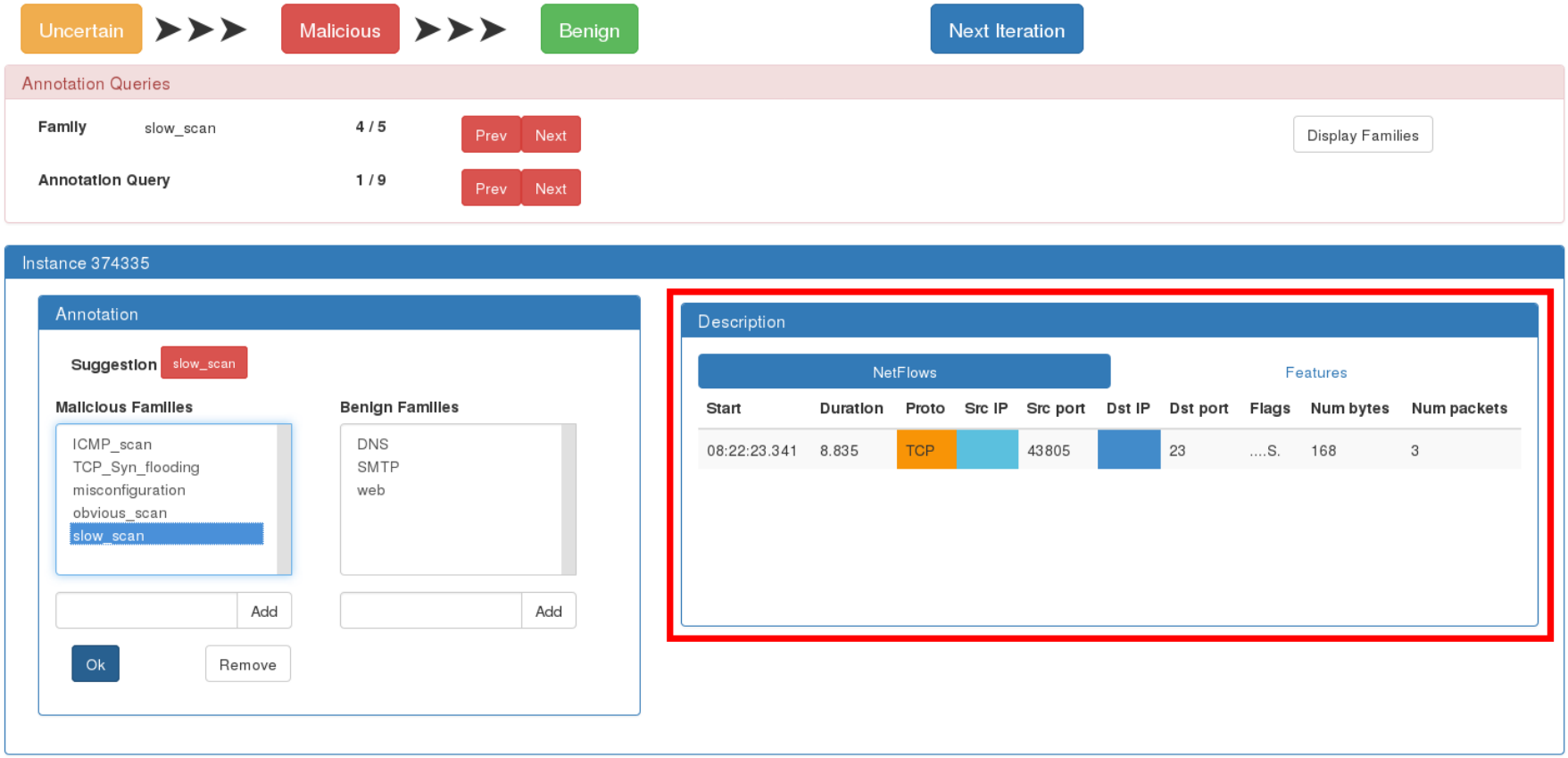
ILAB : système d'annotations

Interface d'annotations



ILAB : système d'annotations

Interface d'annotations



Visualisation(s) spécifique(s)

Afficher tout type de données

NetFlow

Description

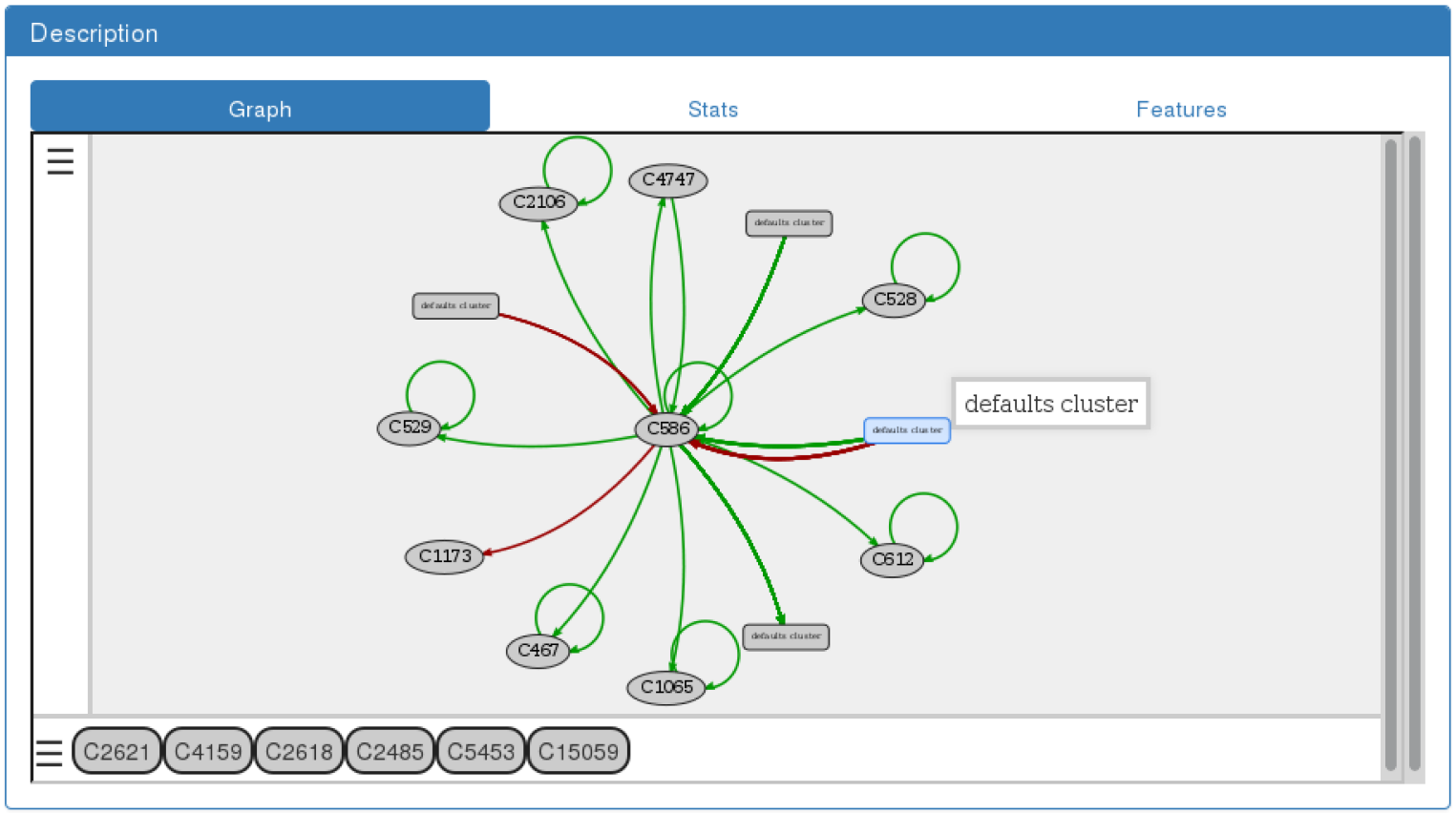
NetFlows | Features

Start	Duration	Proto	Src IP	Src port	Dst IP	Dst port	Flags	Num bytes	Num packets
08:22:23.341	8.835	TCP		43805		23	....S.	168	3

Visualisation(s) spécifique(s)

Afficher tout type de données

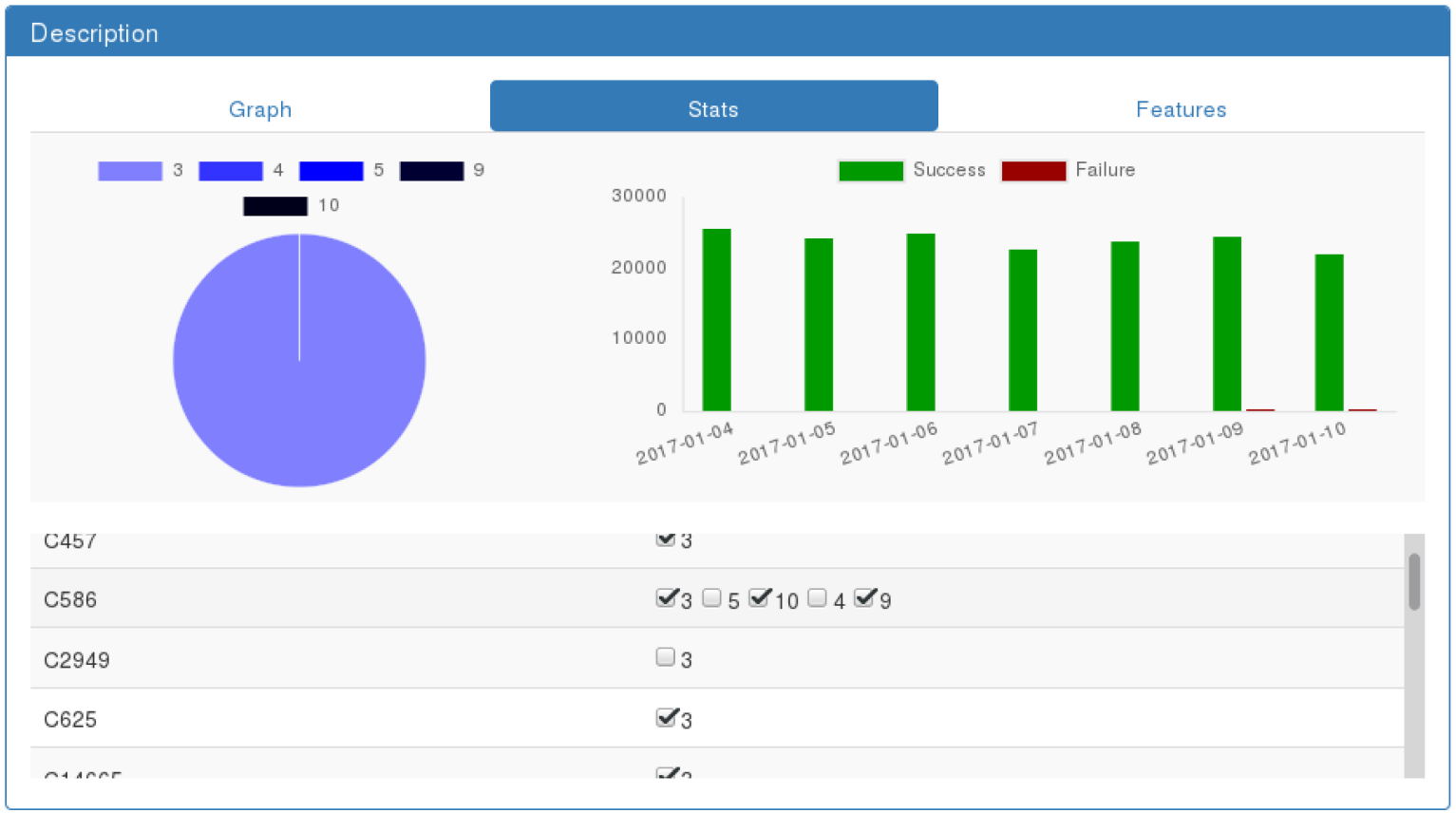
Journaux d'événements Windows



Visualisation(s) spécifique(s)

Afficher tout type de données

Journaux d'événements Windows



ILAB : système d'annotations

Aider l'utilisateur à rester cohérent

Éditeur de familles

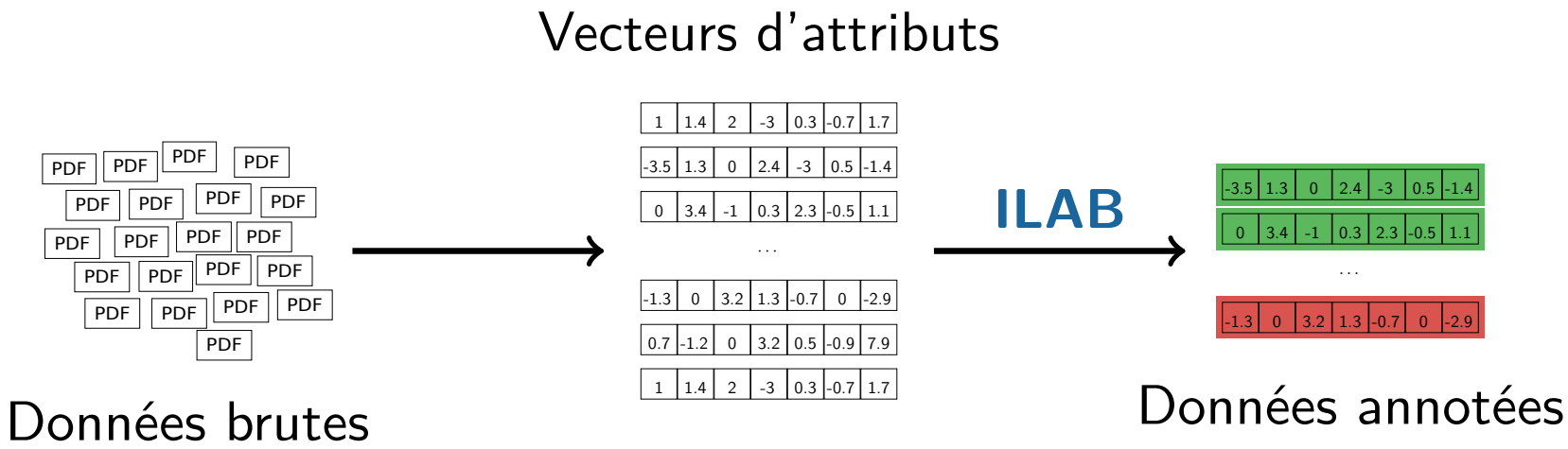
- Changer le nom d'une famille
- Changer le label associé à une famille
- Fusionner des familles

Kulesza et al. Structured labeling for facilitating concept evolution in machine learning, CHI 2014.

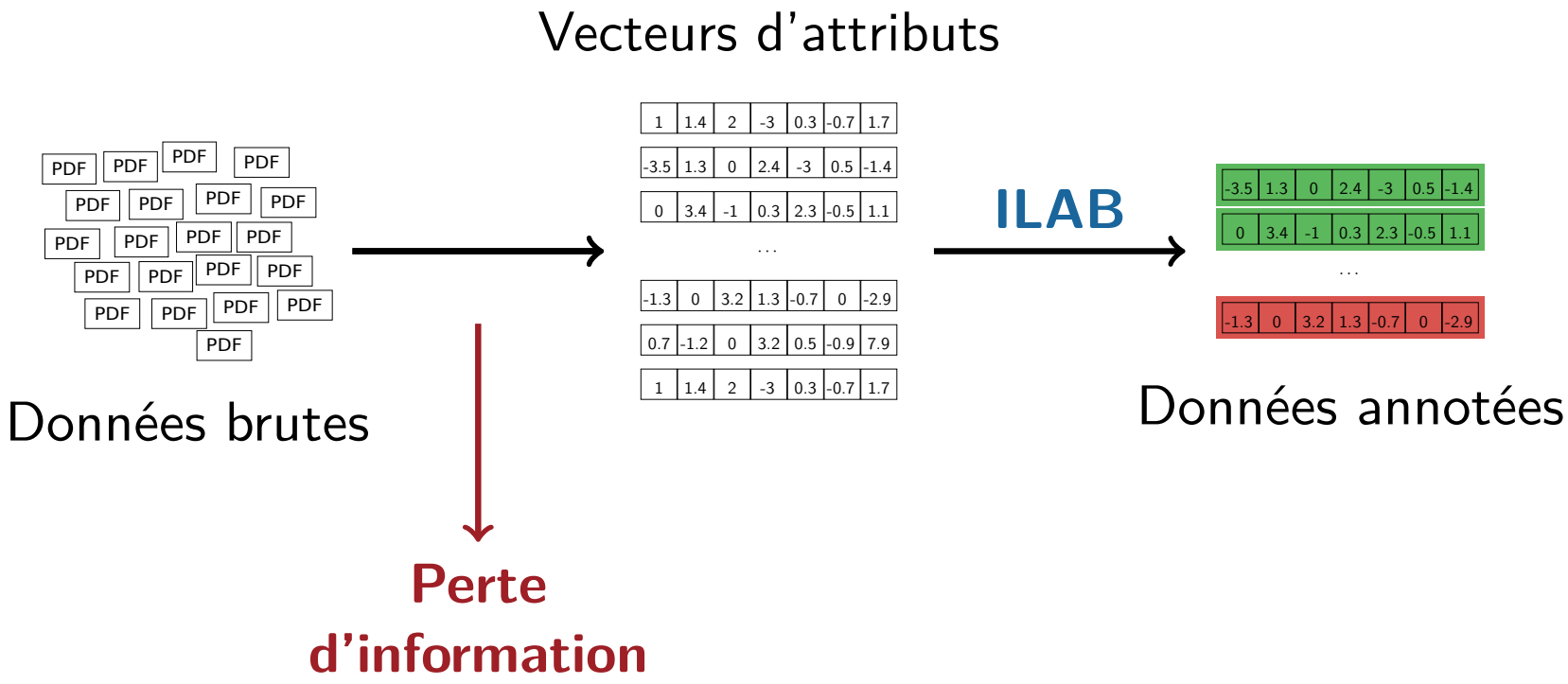
Très utilisé au cours des expériences utilisateur

- Délimitation de la cible de détection
- Définition de la taxonomie des alertes

Lien fort entre les attributs et les annotations



Lien fort entre les attributs et les annotations



Lien fort entre les attributs et les annotations

Les attributs extraits peuvent ne pas être suffisamment expressifs.

Attributs

Nb. octets envoyés/reçus :

- globalement
- sur le port 80
- sur le port 53
- sur le port 25

Annotation

- connexion TCP complète
- sur le **port 22**
- **normale**

Annotation

- connexion TCP complète
- sur le **port 1258**
- **anormale**

Lien fort entre les attributs et les annotations

Connaissance des attributs

- Niveau d'expressivité

Lien fort entre les attributs et les annotations

Solutions

Connaissance des attributs

- Niveau d'expressivité

Faire évoluer les attributs

- manuellement
- ou encore mieux, automatiquement

Khiops Boulle, Towards automatic feature construction for supervised classification, ECML'14.

Featuretools Kanter et al., Deep feature synthesis: towards automating data science endeavors, DSAA' 15.

Hidost Šrndić et al., Hidost: a static machine learning based detector of malicious files, EURASIP'16.

ILAB : Interactive LABelling

Un système d'apprentissage actif complet

Stratégie d'apprentissage actif

- Évite les biais d'échantillonnage
- Maintient un faible temps d'attente

RAID'17 **ILAB: An Interactive Labelling Strategy for Intrusion Detection**

Système d'annotations

- Interface générique d'annotations
- Éditeur de familles

AICS'18, IDEA'18 **End-to-End Active Learning for Computer Security Experts**

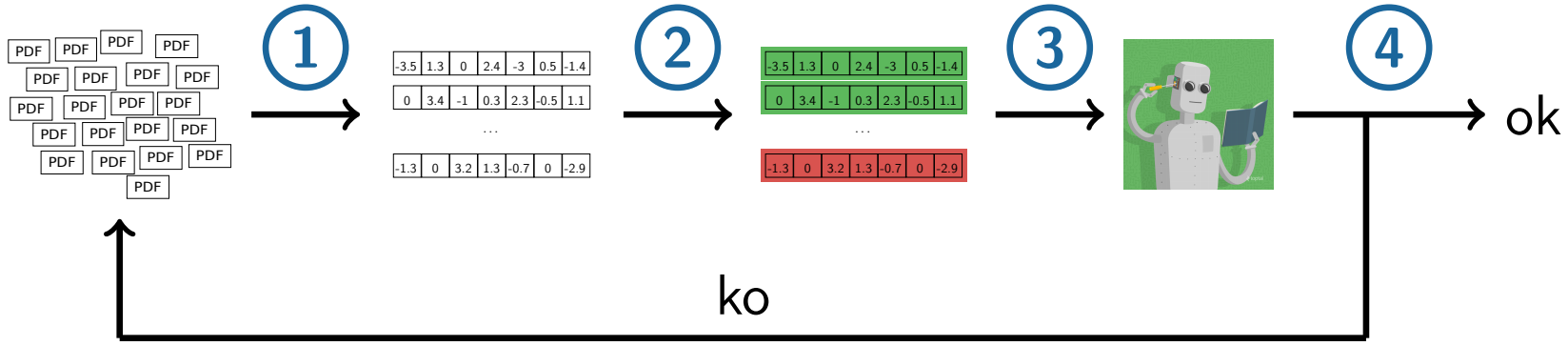
Expériences utilisateur

- Validation des choix de conception
- Pistes d'amélioration

Sommaire

Apprentissage supervisé et systèmes de détection

Une approche de bout-en-bout impliquant les experts en sécurité



1. Extraction d'attributs
2. Annotation
3. Classe de modèles ?
4. Validation

Apprentissage supervisé et systèmes de détection

Une approche de bout-en-bout impliquant les experts en sécurité

Contributions

1. DIADEM : apprentissage et validation d'un modèle de détection
   - **SSTIC'17** — **Le Machine Learning confronté aux contraintes opérationnelles des systèmes de détection**
2. ILAB : annotation d'un jeu de données avec un effort réduit
   - **RAID'17** — **ILAB: An Interactive Labelling Strategy for Intrusion Detection**
   - **AICS'18, IDEA'18** — **End-to-End Active Learning for Computer Security Experts**
3. Génération automatique d'attributs

https://github.com/ANSSI-FR/SecuML

Apprentissage supervisé et systèmes de détection

Une approche de bout-en-bout impliquant les experts en sécurité

Contributions

1. DIADEM : apprentissage et validation d'un modèle de détection
   - SSTIC'17 **Le Machine Learning confronté aux contraintes opérationnelles des systèmes de détection**
2. ILAB : annotation d'un jeu de données avec un effort réduit
   - RAID'17 **ILAB: An Interactive Labelling Strategy for Intrusion Detection**
   - AICS'18, IDEA'18 **End-to-End Active Learning for Computer Security Experts**
3. Génération automatique d'attributs

`https://github.com/ANSSI-FR/SecuML`

Pistes pour la suite

- Améliorer la génération automatique d'attributs

Apprentissage supervisé et systèmes de détection

Une approche de bout-en-bout impliquant les experts en sécurité

Contributions

1. DIADEM : apprentissage et validation d'un modèle de détection
   - SSTIC'17 **Le Machine Learning confronté aux contraintes opérationnelles des systèmes de détection**
2. ILAB : annotation d'un jeu de données avec un effort réduit
   - RAID'17 **ILAB: An Interactive Labelling Strategy for Intrusion Detection**
   - AICS'18, IDEA'18 **End-to-End Active Learning for Computer Security Experts**
3. Génération automatique d'attributs

`https://github.com/ANSSI-FR/SecuML`

Pistes pour la suite

- Améliorer la génération automatique d'attributs
- Faire évoluer les attributs au cours des projets d'annotations

Apprentissage supervisé et systèmes de détection

Une approche de bout-en-bout impliquant les experts en sécurité

Contributions

1. DIADEM : apprentissage et validation d'un modèle de détection
   - SSTIC'17 **Le Machine Learning confronté aux contraintes opérationnelles des systèmes de détection**
2. ILAB : annotation d'un jeu de données avec un effort réduit
   - RAID'17 **ILAB: An Interactive Labelling Strategy for Intrusion Detection**
   - AICS'18, IDEA'18 **End-to-End Active Learning for Computer Security Experts**
3. Génération automatique d'attributs

`https://github.com/ANSSI-FR/SecuML`

Pistes pour la suite

- Améliorer la génération automatique d'attributs
- Faire évoluer les attributs au cours des projets d'annotations
- Rendre les modèles de détection plus robustes