Graph-based Learning and Analysis for intrusion Detection in Information Systems

GLADIS

anr agence nationale de la recherche

Appel : Blanc

Année : 2020

Instrument : PRCi

Contact : haddad@liris.cnrs.fr

COORDINATEUR : Mohammed Haddad, LIRIS – Univ. Lyon 1 PARTENAIRES : SnT, Univ. Luxembourg

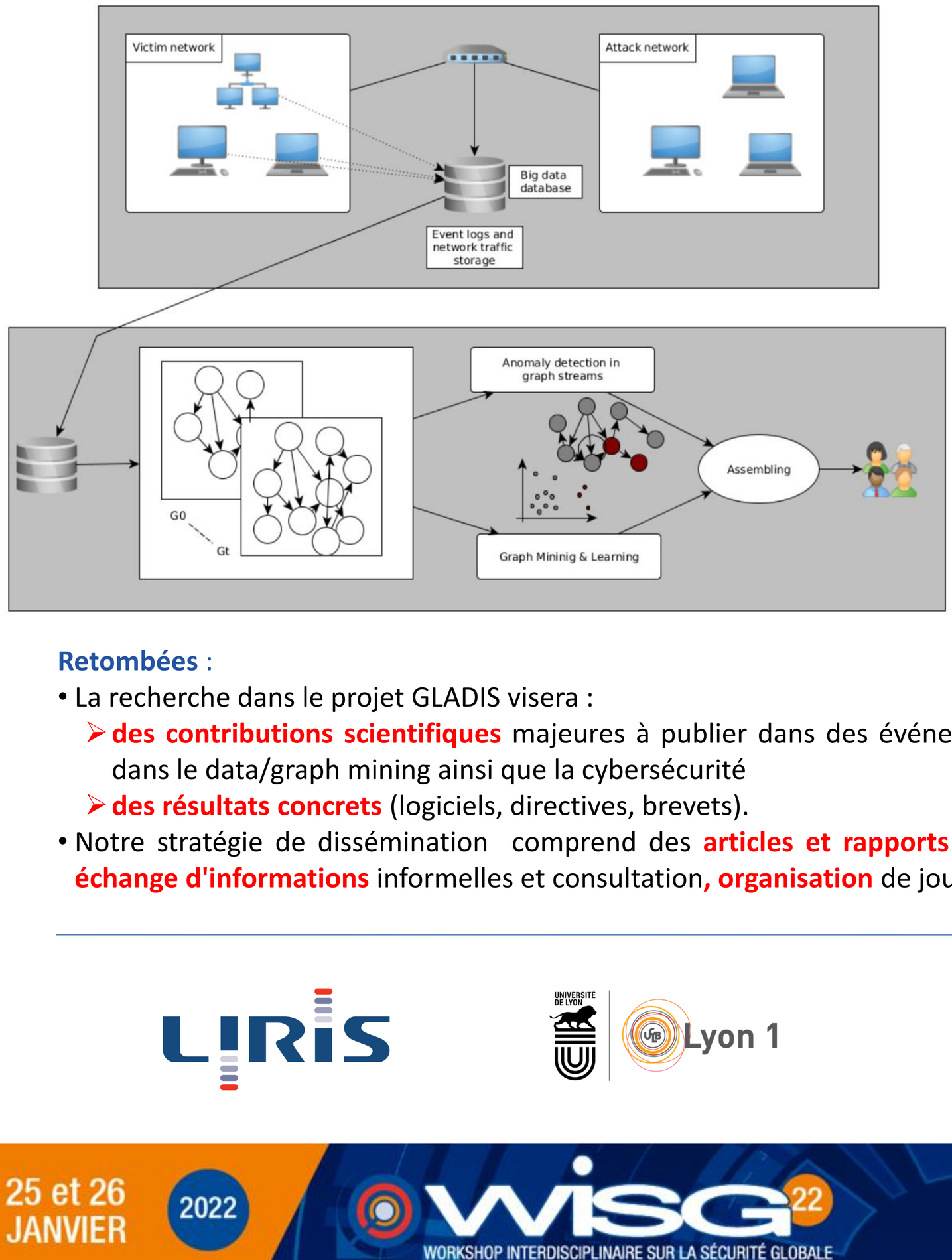
Résumé :
GLADIS vise à construire un système efficace de détection de cyberattaques en temps réel basé sur une représentation graphes des activités du système. Le but du projet est d'identifier les anomalies et de retracer les sources des attaques en utilisant des techniques d'analyse et d'apprentissage de graphes en mode flux.

CONTEXTE ET OBJECTIFS

- Les **cyberattaques** sont aujourd'hui **imprévisibles** et leur détection est un véritable défi car les attaques deviennent de plus en plus **sophistiquées et complexes**.
- La plupart des solutions de surveillance (monitoring) existantes ne peuvent pas faire face à des attaques inconnues et complexes.

➡ **Besoin = détection** en amont **+ prédiction** des comportements malveillants

MÉTHODOLOGIE ET RÉSULTATS



Objectifs :

Les **principaux défis** à relever dans le projet GLADIS pourraient être résumés comme suit:

1. **Améliorer la détection** en augmentant les vrais positifs tout en diminuant les faux positifs.
2. **Améliorer la complexité** de la détection
3. **Apprendre à détecter** des attaques plus sophistiquées dans un délai raisonnable ou, dans le meilleur des cas, en temps réel.
4. **Augmenter la connaissance de l'expert,** *i.e.,* mettre l'expert au cœur du dispositif d'apprentissage et de détection.

➔Modèles à base de **théorie des graphes**

Retombées :

- La recherche dans le projet GLADIS visera :
  - **des contributions scientifiques** majeures à publier dans des événements hautement reconnus (conférences, revues) dans le data/graph mining ainsi que la cybersécurité
  - **des résultats concrets** (logiciels, directives, brevets).
- Notre stratégie de dissémination comprend des **articles et rapports publiés**, des conférences et **réunions publiques**, **échange d'informations** informelles et consultation**, organisation** de journées thématiques, **workshops** …

LIRIS — Université de Lyon — Lyon 1 — SnT securityandtrust.lu — uni.lu Université du Luxembourg