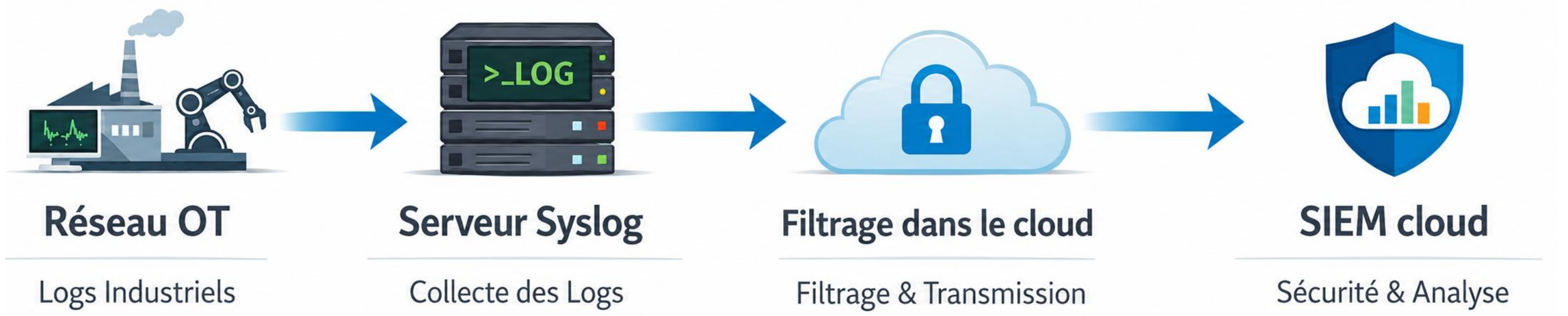
Cartographie des attaques cyber et amélioration de la détection grâce aux produits Schneider Electric

Auteurs : COULIBALY ZIE – POUZENS PAUL - CHEIKHNA MOHAMED TAGHIOULLAH Vatimetou

CONTEXTE ET OBJECTIF

Dans un contexte de menaces cyber croissantes sur les systèmes industriels, Schneider Electric souhaite mieux comprendre les vecteurs d'attaque auxquels ses clients sont exposés, et améliorer la pertinence de ses capacités de détection. Ce projet s'inscrit dans une démarche de cybersécurité proactive, en lien avec les équipes internes du **Managed Security Services (MSS OT)** et les laboratoires d'innovation.

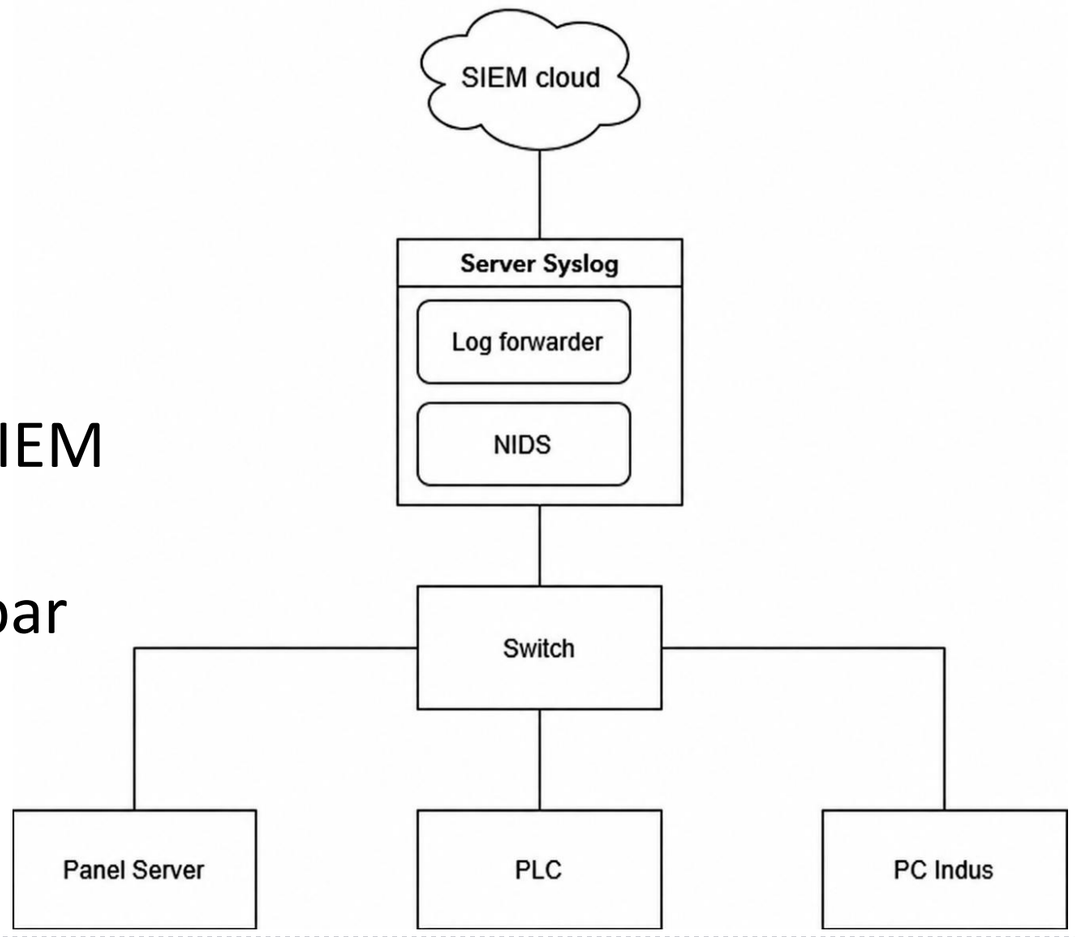
MÉTHODES ET DÉVELOPPEMENTS



L'organisation du projet s'est appuyé sur la méthode agile SCRUM qui a permit de faire des retours rapides sur les livrables. Le but était de remonter les logs des équipements clients Schneider vers un SIEM afin de centraliser la supervision de tous les produits Schneider et de facilement détecter les attaques sur ceux-ci.

RÉSULTATS ET CONCLUSION

- Rapport d'évaluation de la capacité de détection grâce aux frameworks MITRE ATTACK et DETT&CT
- Corrélation et remontée des logs vers le SIEM
- Règles de détection d'attaques.
- Rapport d'amélioration des logs générés par les produits.



MOTS-CLÉS : SIEM/MSS OT/MITRE ATTACK,DETTECT/SCRUM