Training

Detection

Utility Server

Client₁ Client₂ Clientₙ

Word2vec₁ Word2vec₂ Word2vecₙ

Semantic Aggregation $M_{w2v-harm}$

Extract Process Categories $\psi(p)$

Client₁ Client₂ Clientₙ

Central Server

Client₁ Client₂ Clientₙ

$\{GNN_1,...,GNN_{Kcat}\}_1$ $\{GNN_1,...,GNN_{Kcat}\}_N$

$\{GNN_1,...,GNN_{Kcat}\}_2$

Encryption Keys

Federated Averaging GNN_{global}

Client₁ Client₂ Clientₙ

Client Side (Clientₙ)

System Logs

Train Semantic Encoder

Encryption Keys

Provenance Graph $\texttt{PGClient}_N$

Encrypt Tokens

Categorization $\psi(p)$

Harmonization $M_{w2v-harm}$

$\{GNN_1,...,GNN_{Kcat}\}_N$

Client Side (Clientₙ)

System Logs

Provenance Graph $\texttt{PGClient}_N$

Featurization

GNN based Anomaly Detection

Threat Alerts