Thalès

Cybersécurité / Industrie

ANTICIPER LES ATTAQUES SUR SES AVIONS GRÂCE À UNE ANALYSE DES ÉCHANGES ENTRE COMPOSANTS EMBARQUÉS EN VOL.

Le département de cybersécurité de Thalès Avionics a approché LumenAi lors d'un forum DGA à Bordeaux. Thalès s'est intéressé à l'approche entièrement non-supervisée de LumenAI (analyse de graphes à haute fréquence).

L'objectif est de prédire et de **détecter des nouvelles attaques informatiques non référencés** au sein du département de Cybersécurité de Thalès.

SOLUTIONS / APPROCHES :

LumenAI propose de modéliser les échanges entre composants à l'aide de graphes dynamiques haute fréquence. L'approche consiste à résumer l'information du graphe lors du fonctionnement nominal dy système et ainsi **créer des alertes dès que le système dérive.**

RÉSULTATS :

Les algorithmes développés ont **permis de détecter des attaques simulées par des experts cyber-sécurité** avec un taux de faux négatifs inférieur à 10% et un taux de faux positifs équivalent.

De plus, par une approche entièrement non-supervisée, une détection de nouvelles attaques a été mise en place et a permis d'anticiper ces attaques sur plusieurs scénarios d'utilisations.

https://www.lumenai.fr/etudes-cas-client/cybersecurite/thales/

Naval Group

Cybersécurité / Industrie

CYBERSÉCURITÉ : DÉTECTER DES ATTAQUES INFORMATIQUES À PARTIR DES FICHIERS DE LOGS.

L'enjeu pour Naval Group est de sécuriser leurs systèmes embarqués dans leurs navires, afin d'identifier et de contrer les cybers menaces connues ou inconnues.

Naval Group a fait appel à LumenAI pour sécuriser leur système d'information.

Une simulation d'attaque a été introduite dans leur réseau. L'objectif de LumenAI était de détecter le moment de l'intrusion, au travers de fichiers de logs sous format texte.

Ce sont en particulier les menaces inconnues qui ont été traitées durant ce projet.

SOLUTIONS / APPROCHES :

Une équipe projet LumenAI a été mise en place pour traiter l'information par l'étude de la **fréquence des événements et leur ordre d'apparition**, et par la prise en compte de la forme des messages.

LumenAI **a détecté la période de fonctionnement perturbée** qui précèdait l'attaque et a mis en lumière des **activités anormales,** des évènements marquants dont le moment précis de l'attaque

RÉSULTATS :

Livrables :

Des POC pour chaque approche avec du code documenté et la présentation des résultats.

Un document de synthèse de la mission effectuée ainsi que des axes d'améliorations et d'évolutions.

Une **formation aux techniques de Machine Learning** a été réalisée sur site afin de partager notre expertise en cybersécurité.

https://www.lumenai.fr/etudes-cas-client/cybersecurite/naval-group/

IDECSI

IDECSI
Enterprise Security

Cybersécurité / Editeur

INTÉGRER DES SOLUTIONS DE MACHINE LEARNING DANS SON SYSTÈME DE MONITORING ET D'ALERTING.

IDECSI est une startup qui développe un logiciel de cybersécurité capable de détecter des comportements anormaux dans les systèmes d'informations des grandes entreprises.

Pour améliorer les performances de son produit, IDECSI souhaite intégrer des solutions de machine learning dans son système de monitoring et d'alerting.

LumenAI est intervenu sur **un cas client précis**, par une approche de **détection de communautés** dans des graphes dynamiques.

L'étude a consisté à détecter des comportements anormaux, dans un jeu de données (consultation des fichiers par l'ensemble des employés de l'entreprise)

SOLUTIONS / APPROCHES :

LumenAI a proposé de modéliser ce jeu de données par un **graphe où chaque employé est en lien avec les fichiers qu'il a consulté**. Cette modélisation permet de **détecter des groupes de comportements** distincts parmis les salariés, correspondant à leur statut dans la hiérarchie de l'entreprise.

RÉSULTATS :

LumenAI a mis en lumière des comportements **de groupes d'individus « normaux » et anormaux** suite à la mise en œuvre de ses algorithmes. Pour des raisons de confidentialité, la pertinence des résultats ne nous a pas été communiquée.

https://www.lumenai.fr/etudes-cas-client/cybersecurite/idecsi/