GLIMPS
Malware Detect

DATA SHEET

Protection des fichiers, Détection augmentée, Automatisation de l'analyse

Une technologie unique : le Deep Engine

Fort de l'expertise de plus de 10 ans de ses co-fondateurs dans l'IA et le *reverse engineering*, GLIMPS est le spécialiste de l'analyse profonde de fichiers en vue de détecter et de caractériser les menaces les plus sophistiquées en quelques secondes.

GLIMPS a développé une technologie unique qui se différencie des techniques traditionnelles de détection en se focalisant sur l'analyse du code. Son moteur d'Intelligence Artificielle basé sur le *Deep Learning* permet de détecter toute forme de *Malware* au sein de tout type de fichier par comparaison de code. Cette technologie est reconnue scientifiquement, appelée : Conceptualisation de Code

Contexte

A l'heure où les entreprises et les administrations sont confrontées à des menaces de plus en plus sophistiquées et à une diversification des surfaces d'attaques (mobilité, applications collaboratives et métiers, transformation numérique,...), il devient impératif de se doter d'outils performants. Au premier trimestre 2023, 562,4 millions d'e-mails de phishing ont été détectés, soit 284,8 millions de plus qu'au trimestre précédent [Source : VadeSecure]. Depuis 2020, la hausse des cyberattaques a ainsi cru de 400% en France, le coût financier moyen d'une cyberattaque étant compris entre 50 et 500 K€ [Sources : Hiscox, Cisco].

Trop de solutions spécialisées chacune dans leur technologie de détection font perdre du temps aux analystes, à la recherche d'un outil transparent, globalisé et automatisé leur permettant d'optimiser leur MTTD et leur efficience.

Les Bénéfices de GLIMPS Malware Detect

- Détection augmentée multi-moteurs des menaces 0-day, variants, polymorphes, évasives et APT
- Détection des malwares avant qu'ils ne pénètrent dans le SI
- Couverture de toutes les surfaces d'attaque avec une plateforme centralisée
- Prise en charge de tous les formats de fichiers et langages de programmation
- Réduction du Mean Time to Detect (MTTD) - Temps d'analyse des fichiers (inférieur à 3 secondes)

Pour quels cas d'usage ?

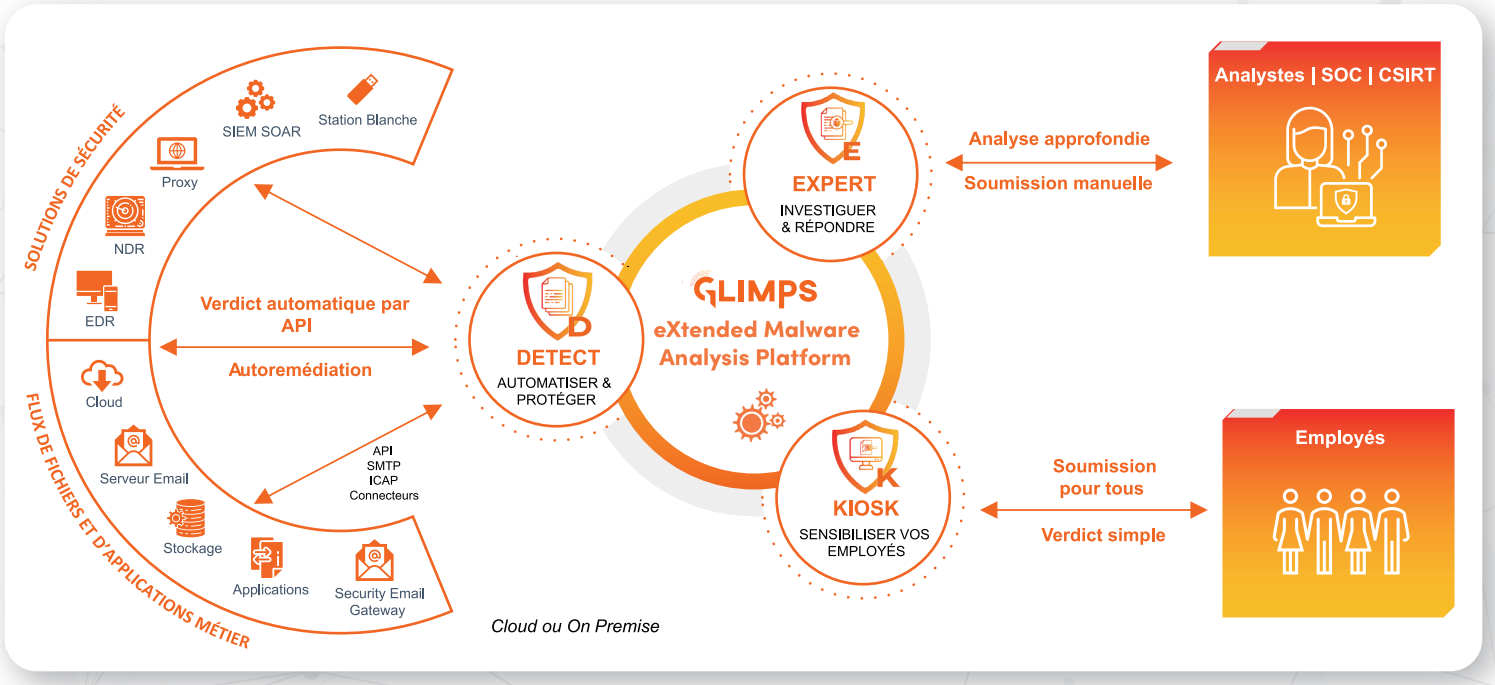
- ☑ Sécurisation des Applications Métiers et Collaboratives
- ☑ Protection des fichiers numériques intégrés aux applications web et cloud
- ☑ Automatisation des processus d'investigation (emails ou fichiers suspects)
- ☑ Détection et qualification augmentées en complément des éléments de sécurité existants (EDR, ESG, WSG, NDR, Bastion, WAAP)

ENHANCED DETECTION PLATFORM

Les fonctionnalités

- Analyse de tout type de fichier avec 25 moteurs d'extraction, d'analyse et de détection statiques
- Capacités d'analyse de larges volumes de fichiers quotidiennement
- Rapport d'analyse synthétique au format JSON (score, familles d'attaquant, résultats des principaux moteurs de détection)
- Interopérabilité avancée grâce à la disponibilité de multiples connecteurs avec les principales solutions IT et cyber du marché
- Intégration simplifiée via API REST, ICAP ou SMTP
- Module d'alertes configurable (par mail, SYSLOG, SPLUNK, MISP)
- Système de cache pour réduire encore le temps d'analyse
- Dashboard de statistiques sur les analyses effectuées

UNE INTÉGRATION SIMPLIFIÉE



Pourquoi choisir GLIMPS Malware Detect ?

- Analyse par *Deep Learning*, technologie d'IA propre à GLIMPS, permettant de caractériser les menaces 0-day, variants, polymorphes, évasives et APTs
- 0 latence : non impactant dans l'expérience utilisateur
- Détection des malwares >99%
- Souveraineté (éditeur français, hébergement en France et Europe) et protection des données soumises en environnement fermé (aucune donnée ne sortant de la plateforme)
- Possibilité d'un déploiement facile en *SaaS* et *On-prem avec mêmes* fonctionnalités et performances

demo@glimps.re

GLIMPS

+33 2 44 84 78 44 | www.glimps.re

1179 Avenue des Champs Blancs,
35510 Cesson-Sévigné – France