GLIMPS
Malware Expert

DATA SHEET

Analyse profonde des menaces,
Contextualisation

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. Durant le 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 MTTR et leur efficience.

Les Bénéfices de GLIMPS Malware Expert

- Automatisation de la totalité des tâches de malware forensics et threat hunting
- Identification immédiate du périmètre compromis
- Accélération de l'analyse et de la réponse à incident (diminution du MTTR de 70%)
- Visibilité totale sur les menaces grâce à une plate-forme unique (plateforme all-in-one idéale pour l'analyse de malware)

Pour quels cas d'usage ?

- ☌ Investigation, levée de doute et réponse à incidents (DFIR)
- ☌ Reconstruction du SI
- ☌ Threat Hunting
- ☌ Enrichissement de la CTI

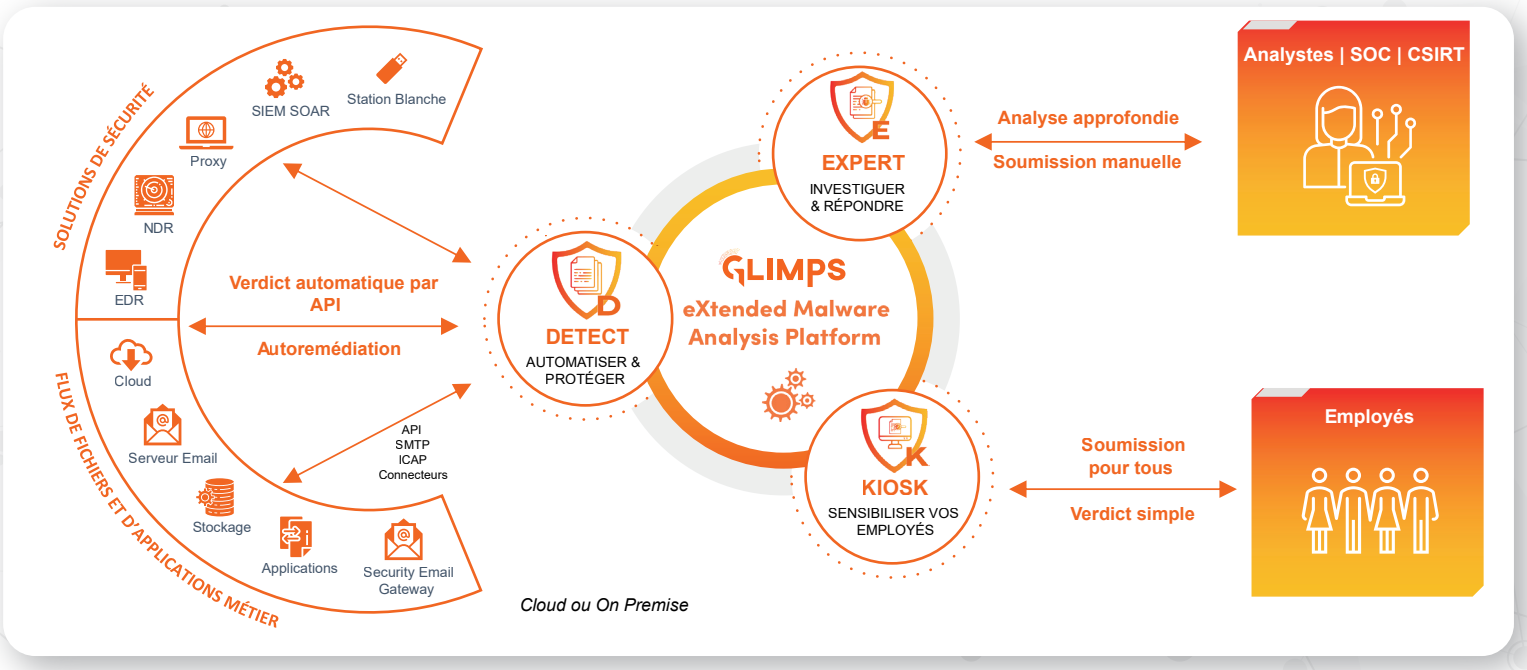
OPEN XDR PLATFORM · CAMPUS CYBER · HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY · FRANCE RELANCE · La FRENCH TECH DEEPNUM20

MALWARE FORENSICS

Les fonctionnalités

- Analyse de tout type de fichier avec 25 moteurs d'extraction, d'analyse et de détection statiques, dynamiques et hybrides
- Consultation des résultats d'analyse de l'ensemble de vos sources de soumissions (GLIMPS Malware Detect et GLIMPS Malware Kiosk)
- Analyse précise et fonctionnelle de la menace en temps réel et aide à la décision grâce à la contextualisation
- Prévisualisation sûre des documents sans avoir à les ouvrir sur votre poste
- Extraction des informations des malwares : familles d'attaquant, fonctions malveillantes, IOCs, Mitre Attack mapping
- Statistiques, rapports et exports multiformats (pdf, misp, stix, json,...)
- Conforme au RGPD / Rétention des données et des analyses paramétrables
- Module d'alertes configurable (par mail, SYSLOG, SPLUNK, MISP)
- Editeur YARA et capacité de retro hunting sur votre historique de soumissions
- Whitelist et dataset de malwares privés

UNE INTÉGRATION SIMPLIFIÉE



Pourquoi choisir GLIMPS Malware Expert ?

- Analyse par *Deep Learning*, technologie d'IA propre à GLIMPS, permettant de caractériser les menaces 0-day, variants, polymorphes, évasives et APTs
- 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 perfomances
- Accessible à tous les niveaux d'expertise des équipes SOC/CERT

demo@glimps.re

GLIMPS

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

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