

GORILLE EXPERT

AUTOMATISER L'ANALYSE FORENSIC

GORILLE Expert est une solution de cybersécurité complète et précise pour l'analyse et la caractérisation de menaces informatiques. Cette solution analyse minutieusement les fichiers binaires exécutables suspects récupérés (post-incident ou en cas de simple suspicion) et les compare à d'autres binaires. Son fonctionnement statique et dynamique permet de caractériser de nouvelles souches de logiciels malveillants afin de réparer les dégâts causés par une attaque.

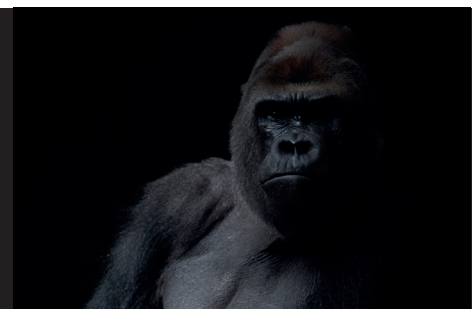
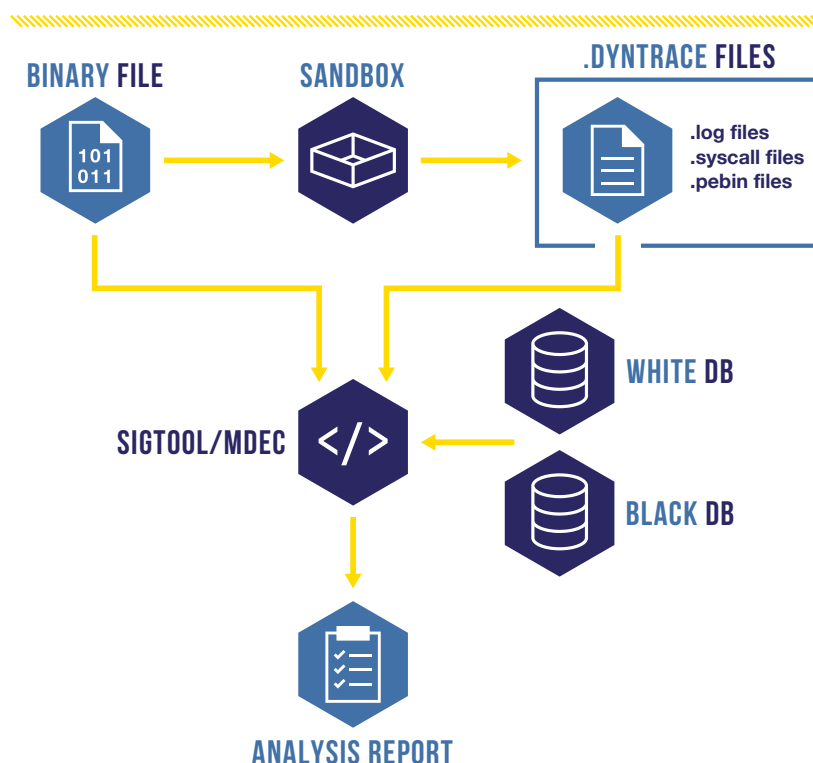
LA SOLUTION LOGICIELLE

GORILLE Expert est un service de détection et d'analyse des menaces informatiques. La suite de logiciels GORILLE Expert, grâce à la technique d'analyse morphologique, permet l'automatisation de l'analyse forensic, le désassemblage des malwares détectés et la caractérisation de codes malveillants. GORILLE Expert permet une double analyse :

- une analyse statique qui permet la construction d'un flot de contrôle (CFG),
- une analyse dynamique, via l'exécution dans une sandbox, permettant de récupérer une trace d'exécution pour aider à la construction du CFG du binaire et de contourner l'obfuscation et les packers.

Également utile pour la rétro-ingénierie la solution vous permet de créer vos propres bases de données pour analyser et comparer des binaires.

Maîtriser les interfaces en lignes de commande et avoir des compétences en analyse de binaires sont nécessaires pour utiliser cette solution. Pour la fonctionnalité d'analyse dynamique, la mise en place d'un environnement d'exécution du binaire est requise (VMware, VM Windows).



AVANTAGES DE LA SOLUTION GORILLE EXPERT

- 🔑 double analyse statique et dynamique
- 🔑 comparaison de binaires
- 🔑 résistance aux packers et obfuscations
- 🔑 interfaçable avec IDA et tout autre désassembleur
- 🔑 facilement scriptable pour s'intégrer dans votre process métier
- 🔑 génération de bases de données de logiciels malveillants déjà analysés
- 🔑 rapidité de désassemblage
- 🔑 facilité d'installation
- 🔑 solution entièrement paramétrable
- 🔑 re-synchronisation du code pour détection de fonctionnalités / comportements
- 🔑 sans effet indésirable sur le endpoint : l'analyse se fait en mode protégé au sein d'une machine virtuelle et non sur le poste utilisateur

L'ANALYSE MORPHOLOGIQUE, FORCE EXCEPTIONNELLE DE GORILLE

GORILLE se base sur notre technologie unique et innovante d'Analyse Morphologique. Cette technologie, mise au point au sein du Laboratoire de Haute Sécurité du LORIA (CNRS, Inria, Université de Lorraine), a été testée et adoptée entre autres par les équipes de la DGA (Direction Générale de l'Armement).

En qualifiant les codes (sites) malveillants ainsi détectés, l'Analyse Morphologique repère des attaques inconnues, sophistiquées ou encore obfusquées.

Combinant l'Intelligence Artificielle (apprentissage de nouvelles menaces, identification de fonctions), les outils de méthodes formelles et les techniques de reverse-engineering (désassemblage, désobfuscation), notre technologie offre une précision unique et inégalée sur les exécutables sans nécessiter de phase d'apprentissage ni tuning local.

Elle analyse dynamiquement (par exécution) et instantanément les fonctionnalités embarquées dans une application.

À la différence des antivirus, GORILLE Expert est capable de détecter des variants indétectés de malwares, et d'anticiper des attaques en analysant des risques potentiels sur une application inconnue. GORILLE a également la capacité d'intégrer immédiatement et automatiquement tout nouveau comportement malveillant afin de détecter les nouvelles menaces.

Nos partenaires



cyber-detect.com

contact@cyber-detect.com

SAS CYBER-DETECT Campus ARTEM 92 rue du Sergent Blandan - 54000 NANCY

03 72 744 972