

GORILLE PATROUILLE

EXTIRPER LES INFECTIONS DÉJÀ DANS VOTRE PARC

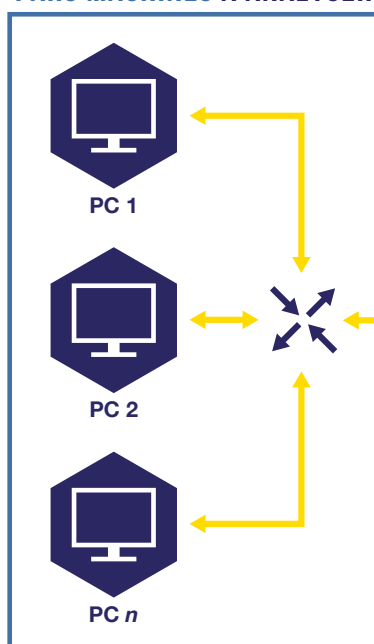
Des attaques ou des menaces peuvent persister dans vos systèmes d'information sans avoir été détectées, et d'autres en provenance de vos partenaires, fournisseurs ou collaborateurs, peuvent infecter votre système d'information et entraîner des arrêts de service.

Pour répondre à ces problématiques et vous garantir la mise en place d'une analyse proactive et automatique, nous avons développé la solution GORILLE Patrouille, qui analyse la totalité de votre parc machines pour détecter d'éventuels binaires exécutables malveillants dormants.

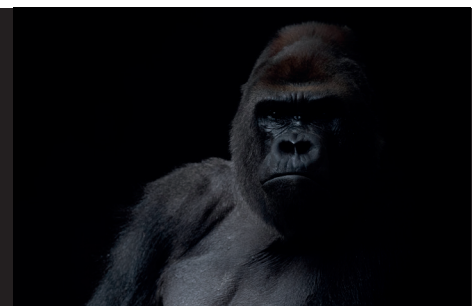
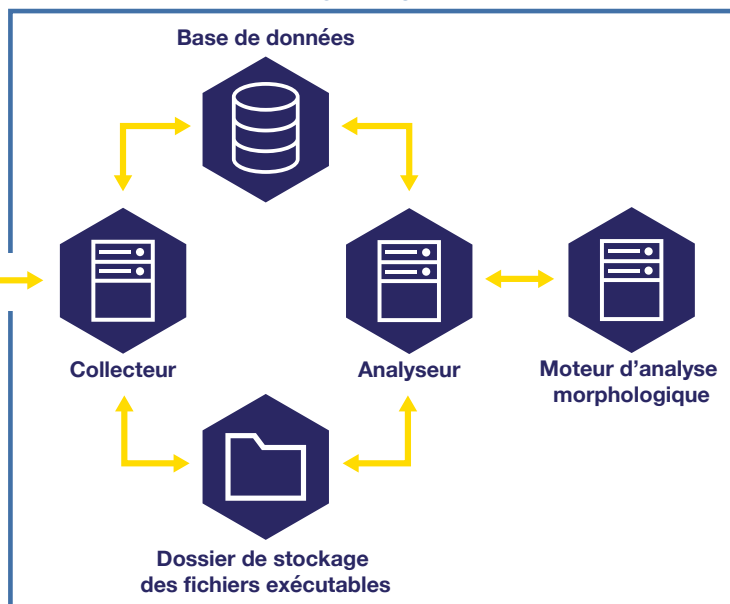
LA SOLUTION LOGICIELLE GORILLE PATROUILLE

GORILLE Patrouille est une suite logicielle permettant de déporter le scan anti-virus d'une machine distante sur un serveur. Un agent scanneur est déployé sur toutes les machines suspectes. L'analyseur est installé sur un serveur et les machines s'y connectent pour soumettre les fichiers. Chaque fichier est analysé grâce à la technologie de GORILLE Expert, basée sur l'analyse morphologique. Les fichiers exécutables système, application, drivers et scripts sont scannés. Un rapport est généré, qui référence les fichiers suspects et identifie les machines infectées pour les isoler.

PARC MACHINES À ANALYSER



SERVEUR



AVANTAGES DE LA SOLUTION GORILLE PATROUILLE

- pas d'impact pour les utilisateurs des machines analysées
- 100% cloud ou on premise
- analyse rapide et simplicité d'utilisation
- pas de bases de données à maintenir
- préserve des effets d'une infection en agissant en amont des exécutions des charges virales qui impactent l'exploitation d'une entreprise
- cohabite avec les antivirus déjà installés tout en demeurant indépendante

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 Patrouille 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