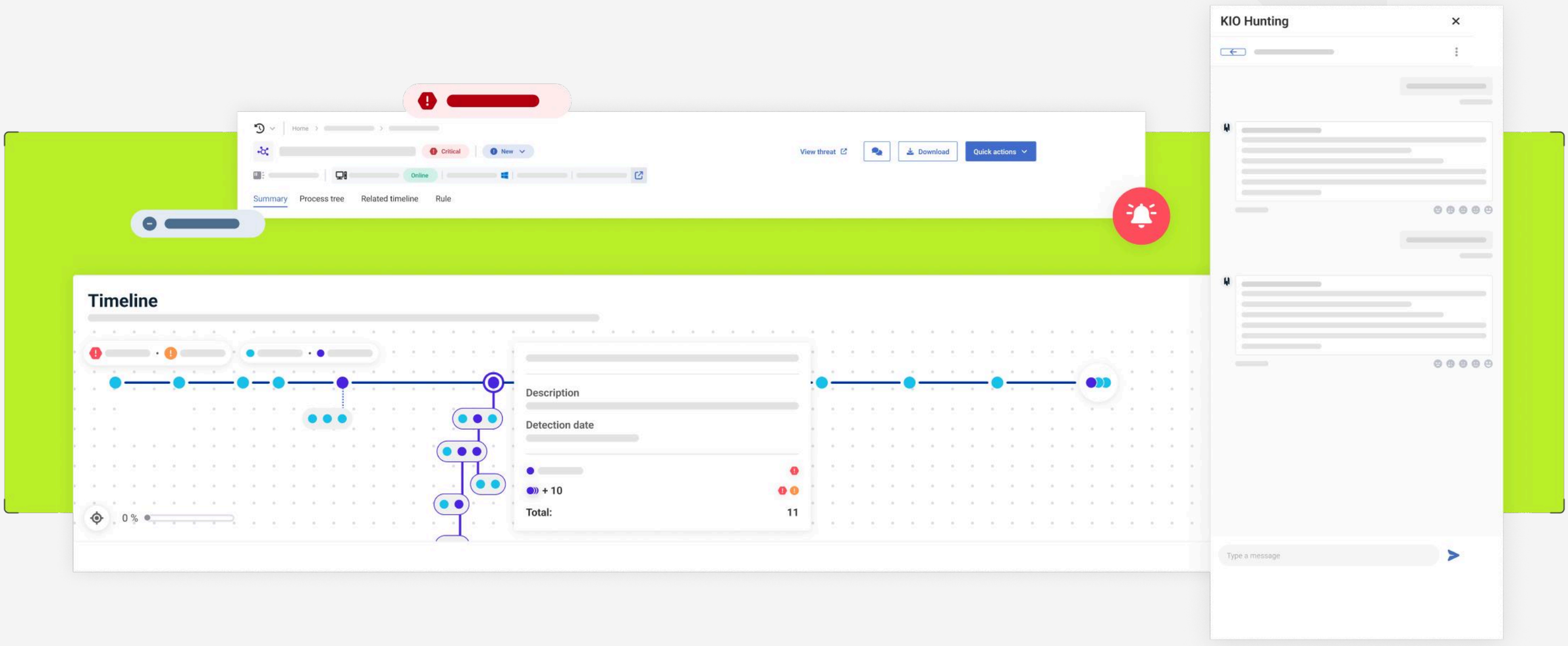
HarfangLab

YOUR ENDPOINTS, OUR PROTECTION

EMPOWER YOUR ANALYSTS, OVERCOME THE THREATS

HarfangLab EDR est une solution de cybersécurité composée d'agents stratégiquement placés sur les terminaux, aussi bien sur les postes de travail que sur les serveurs.

Ces agents communiquent de manière transparente avec un gestionnaire centralisé, orchestrant des capacités de cyberdéfense robustes et en temps réel. Obtenez une compréhension rapide des situations complexes grâce à des fonctionnalités d'enquête et permet une remédiation rapide.



L'AGENT HARFANGLAB, GARDIEN DE VOS ENDPOINTS

L'agent est un élément essentiel de l'EDR, jouant un rôle crucial pour une sécurité à toute épreuve des points finaux, car il fournit une télémétrie **complète au gestionnaire et bloque les menaces identifiées.**

L'agent HarfangLab est conçu sur un profil avancé et léger, **minimisant la consommation de ressources et démontrant une adaptabilité sur les principaux systèmes d'exploitation.** De plus, il intègre une suite de moteurs de détection très efficace, contribuant à une **défense résiliante** contre l'évolution des défis de sécurité.

01 ›› **Pas de redémarrage à l'installation et mises à jour**

02 ›› **Politiques communes pour la gestion de flotte**

03 ›› **Performances optimisées (1% besoin CPU/170 Mo de mémoire)**

04 ›› **Windows, Linux et MacOs**

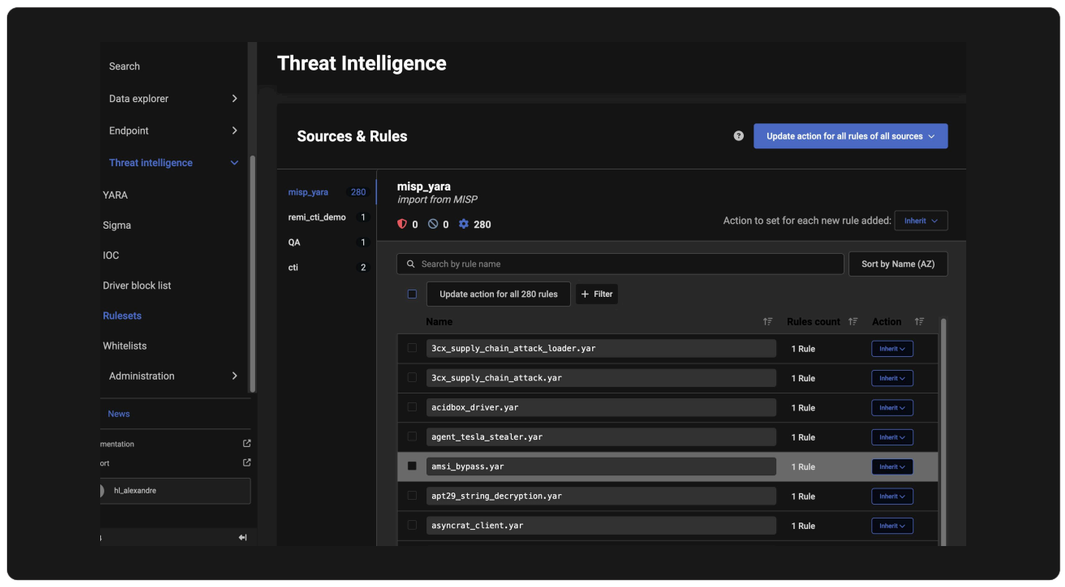
05 ›› **Ordinateurs de bureau et serveurs**

HarfangLab

FONCTIONNALITÉS CLÉS

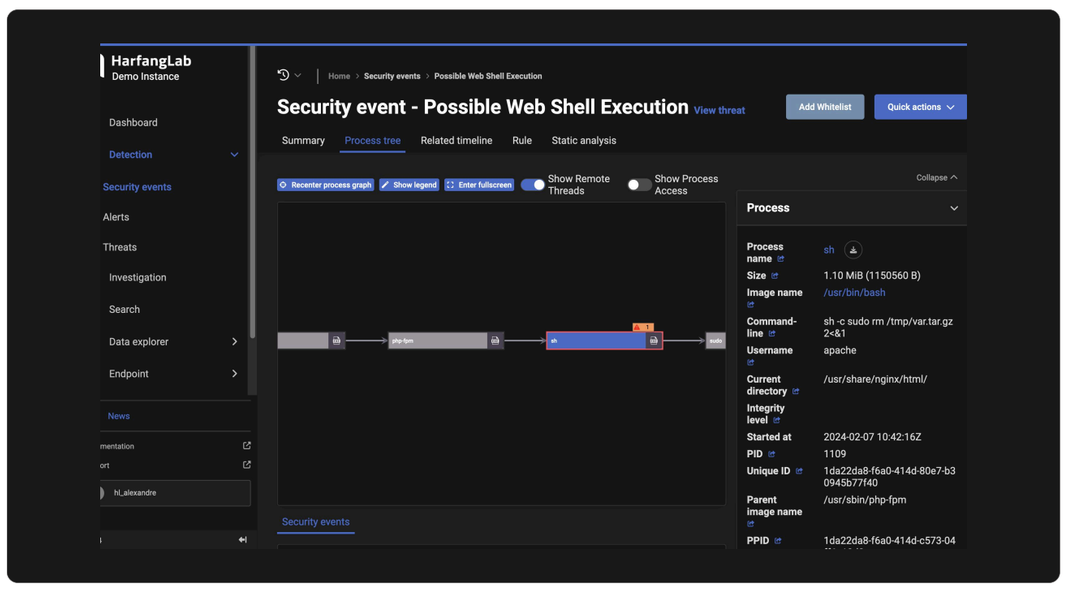
DÉTECTER TOUTES LES MENACES

- Tirez parti de nos moteurs de détection : IoC, Yara, Sigma, AI Binaries & Scripts, Ransomguard
- Détectez les menaces inconnues avec les moteurs d'IA
- Moteurs intégrés sur les agents pour une protection optimale
- Personnalisez vos propres règles de détection.
- File Integrity Monitoring : Vérifier et analyser l'intégrité des fichiers critiques pour détecter toute altération ou corruption possible.



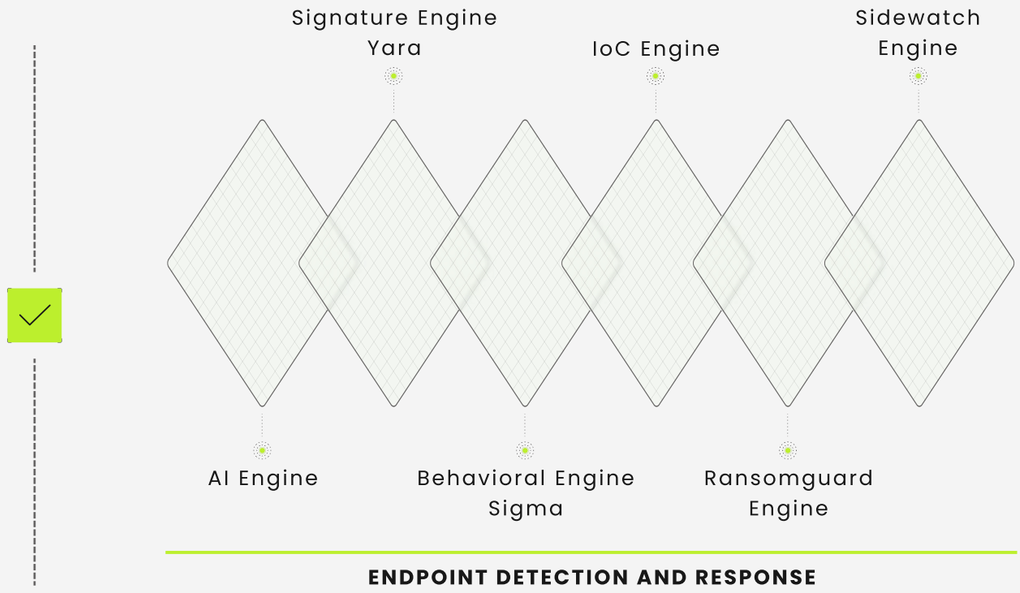
RÉPONSES EN TEMPS RÉEL

- Alertes faciles à traiter
- Flux de données continu avec possibilité de personnaliser les réponses de chaque moteur : on alert, telemetry on alert, alert and block
- Bloquer le processus à l'exécution.



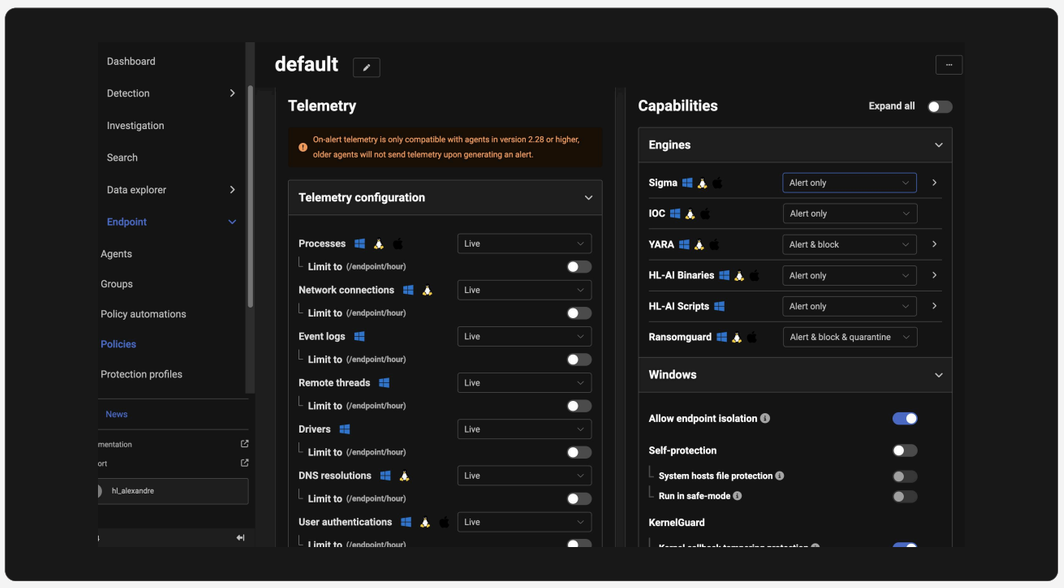
RENFORCEZ VOTRE GESTION DE LA SÉCURITÉ

- Interface intuitive
- Gestion des Whitelists et optimisation des faux positifs
- Déploiement en mode Cloud ou en Infrastructure Privée
- API REST documentée et mise à disposition de connecteurs tiers.



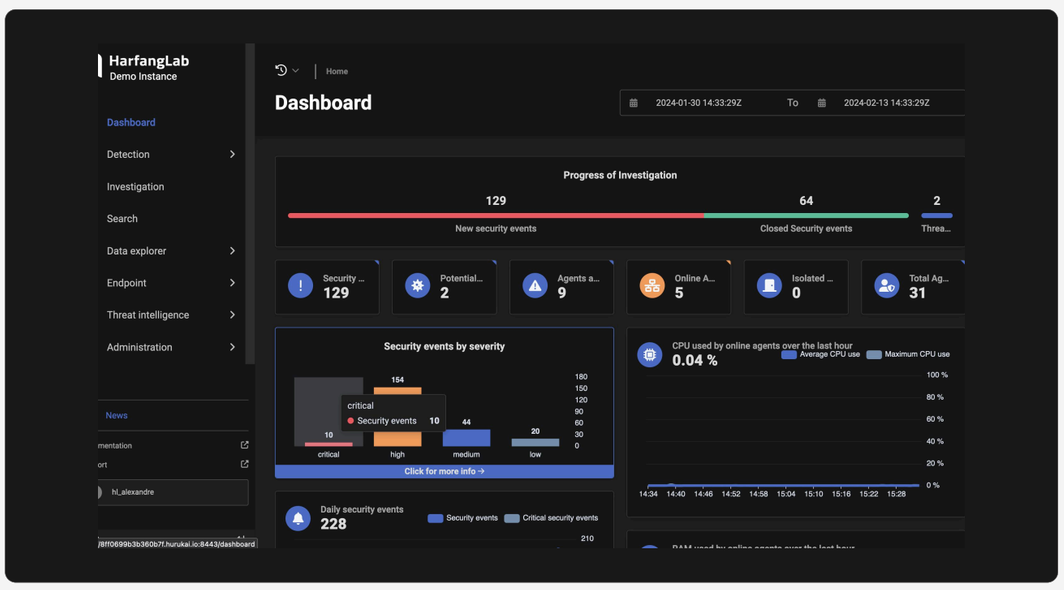
ENRICHISSEMENT CONTINU DES RENSEIGNEMENTS SUR LES MENACES

- Règles et algorithmes de détection élaborés par des experts de haut niveau en cybersécurité
- Amélioration des connaissances à partir de cas d'utilisation des clients, d'échanges avec des partenaires ou d'informations publiques.



ENQUÊTER ET REMÉDIER AUX ÉVÉNEMENTS DE SÉCURITÉ

- Des règles ouvertes pour une meilleure compréhension de l'alerte et une réponse plus rapide
- Outil de Forensic : Graphique en arbre des processus, Data lake
- Lancer des Jobs pour l'investigation et la remédiation des menaces
- Remédiation : isoler le terminal infecté, tuer le processus, supprimer ou mettre en quarantaine des fichiers.



RENFORCEZ VOTRE GESTION DE LA SÉCURITÉ

- Interface intuitive
- Gestion des Whitelists et optimisation des faux positifs
- Déploiement en mode Cloud ou en Infrastructure Privée
- API REST documentée et mise à disposition de connecteurs tiers.

HarfangLab Office
5 rue Feydeau - 75002 Paris

harfanglab.io