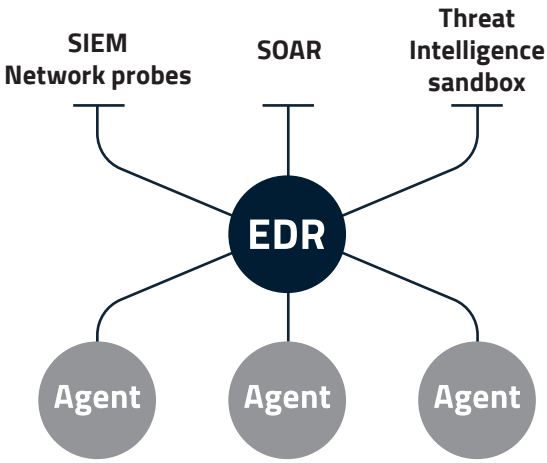
HarfangLab EDR*

Bloquez les cyberattaques, même invisibles.

*EDR: EndPoint Detection & Response

ARCHITECTURE SUR MESURE

La solution est constituée d'agents, déployés sur les terminaux du système et d'un manager central.



AGENTS MULTIPLATFORMES

1. Les interconnexions aux solutions tierces

L'EDR est nativement intégré avec d'autres solution de cybersécurité grâce à une API complète et documentée.

2. Le stockage des données dans les noeuds ElasticSearch

L'EDR HarfangLab peut être déployé dans un cloud choisi par le client ou on premises.

3. Le pilotage des agents déployés sur le parc

Nos agents sont compatibles avec les plateformes :

- Windows 7, 8, 8.1, 10, 11
- Windows server2008 R2, 2012, 2016, 2019
- Ubuntu, Debian, RedHat, CentOS

DETECTION AUTOMATIQUE

HarfangLab EDR collecte les données sur les terminaux
et génère instantanément les alertes, grâce à plusieurs moteurs de détection :

- un moteur gère les règles YARA et les IOC
- un moteur de réputation
- un moteur comportemental basé sur les règles Sigma
- un moteur d'intelligence artificielle basé sur un réseau de neurones

Les moteurs sont activables & paramétrables

HarfangLab EDR

INVESTIGATION APPROFONDIE

La précision dans la qualification de la menace dépend du nombre d'indicateurs explorés.

Les experts sont guidés par des modèles pour :

1. Analyser les menaces inconnues

- Persistance
- Analyse heuristique et statistique
- Compromissions antérieures

2. Lever une suspicion de compromission

- Prélèvement de fichiers
- Capture réseau, mémoire & disque

Acquisition	▪ Capture mémoire d'un processus ou mémoire complète ▪ Extraction de la MFT ou copie d'un disque ▪ Téléchargement d'un fichier ou d'un répertoire ▪ Capture de paquets réseau
Information	▪ Liste des drivers chargés ▪ Liste des processus en cours d'exécution ▪ Liste des pipes nommées ▪ Liste des partages réseau ▪ Liste des sessions ouvertes ▪ Liste des correctifs Windows déployés
Persistance	▪ Les entrées de la base de compatibilité ▪ Les recherches de bootkits dans les secteurs MBR, VBR, IPL ▪ Les ruches Windows ▪ Les tâches planifiées ▪ Les startup files ▪ La base WMI
Evidence	▪ Les fichiers prefetch
Logs	▪ Les journeaux d'événements Windows et Linux

REMEDIATION CIBLEE

Adaptez les règles de remédiation et agissez simultanément sur tout votre parc .

1. Empêcher la propagation d'une menace

- Isolation de terminaux
- Blocage de processus

2. Neutraliser sur les terminaux compromis

- Confinement et arrêt de processus
- Suppression de fichiers
- Nettoyage des bases de registre

contact@harfanglab.fr