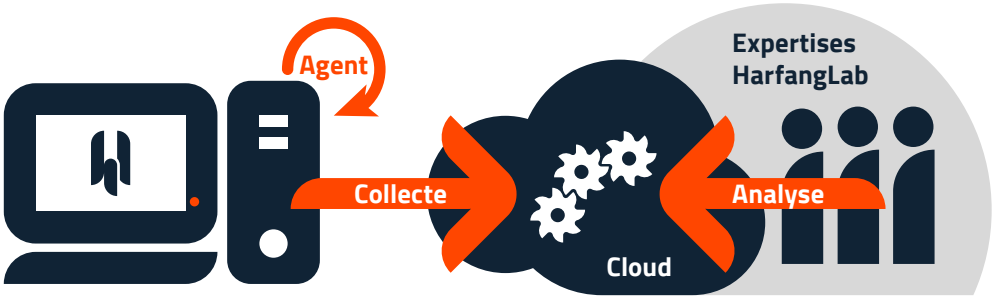
HarfangLab

Grâce à HarfangLab EDR*, détectez les premiers signes de comportements malveillants sur votre parc informatique, et préservez votre entreprise des cyberattaques.

*EDR: EndPoint Detection & Response

ARCHITECTURE GLOBALE



Constitué d'agents déployés sur vos terminaux et d'un manager central déployé en cloud, la solution est entièrement configurable pour s'adapter à votre besoin.

DÉPLOYEZ

1. Déploiement du manageur dans notre instance
Le déploiement du manageur est pris en charge par nos experts.

2. Déploiement des agents dans votre instance
Vous identifiez les terminaux pilotes sur lesquels vous déployez l'agent de l'EDR pour mener vos tests et commencer votre déploiement opérationnel.

Cliquez ici pour découvrir la procédure détaillée de déploiement des agents

CONFIGUREZ

1. Configuration du manager
Vous interconnectez votre EDR à d'autres solutions comme votre SIEM ou une base de Threat Intelligence. Par défaut, vous bénéficiez de la connexion à notre flux de Threat Intelligence.

Cliquez ici pour découvrir les possibilités de configuration du manager

2. Configuration des agents
Vous pouvez regrouper vos agents en groupes, auxquels vous attribuez des politiques de sécurité, qui définiront le comportement des agents.
Rendez -vous dans le menu « Endpoints » pour créer vos groupe et gérer les politiques associées.

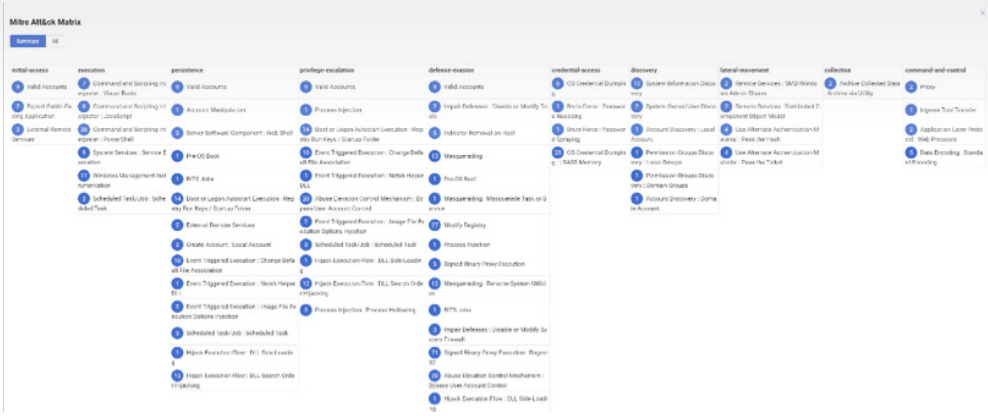
Cliquez ici pour découvrir comment paramétrer vos agents

HarfangLab

ANALYSEZ

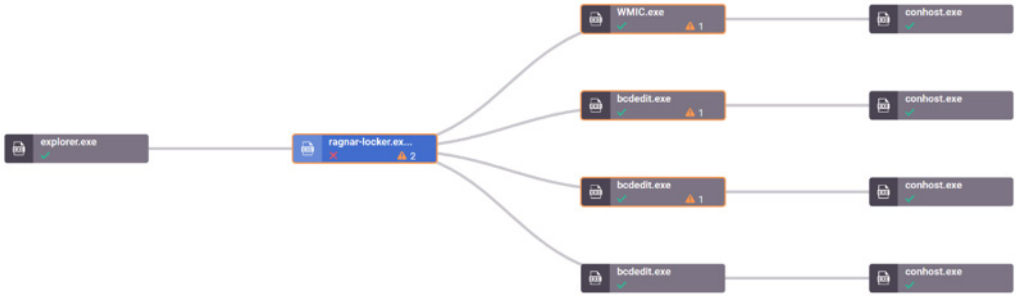
1. L'état global du parc

Rendez-vous dans le menu « Alerts » pour visualiser et gérer les alertes de sécurité.
Vous accédez à une représentation de l'ensemble des alertes dans la matrice Mitre ATT&CK selon le niveau de menace pour mieux prioriser le traitement et voir en un instant le risque opérationnel.



2. Une alerte en profondeur

Accéder au détail d'une alerte en cliquant sur le bouton :



Analyser jusqu'à chaque évènement composant l'alerte
et accéder au contexte d'exécution des processus.

Cliquez ici pour en savoir plus sur la vue détaillée d'un évènement de sécurité.

INVESTIGUEZ

Mener des recherches approfondies

À l'aide de job d'investigation, mener des campagnes de recherche de compromission et décortiquer l'état de santé de chacun de vos terminaux