Installation et configuration EPDR

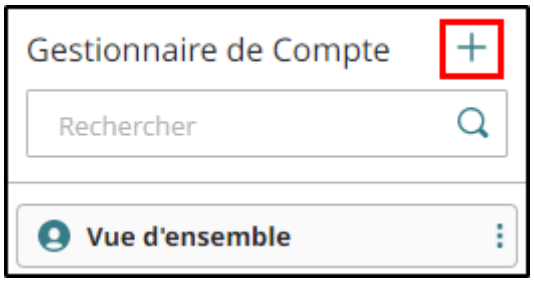
Ici on va aborder l'installation « basique » de l'EPDR WatchGuard, une installation qui permettra de protéger correctement le client, sans aborder la partie spécifique de l'EPDR.

Il faut prévoir un peu de temps avant installation pour préparer au mieux l'arborescence et la méthode d'installation du logiciel.

Préparation du compte client :

Rendez-vous sur le portail WatchGuard cloud : https://cloud.watchguard.com

Connectez vous avec vos identifiants. Une fois connecté si le client n'existe pas, ajoutez-le :



Si le compte vient d'être créé, vous aurez le choix d'allouer directement une licence Endpoint sur la page d'accueil.

Si jamais le client existe déjà, placez-vous sur l'onglet « Vue d'ensemble » puis dans « Inventaire » et enfin l'onglet « Allocation sous Endpoint.

Dans ce menu, vous allez retrouver les licences qui sont allouées, non allouée disponibles ou non. Cliquez sur Allouer des Endpoints :

Dans ce menu vous allez pouvoir définir le nom du client, sélectionner le type de produit et sa quantité. Vous pouvez aussi ajouter des modules, et définir la date d'expiration à **3 ans** à partir de l'installation.

Enfin vous pouvez cliquer sur enregistrer. Si vous n'avez pas de licences disponibles assurez vous qu'elles aient bien été commandées.

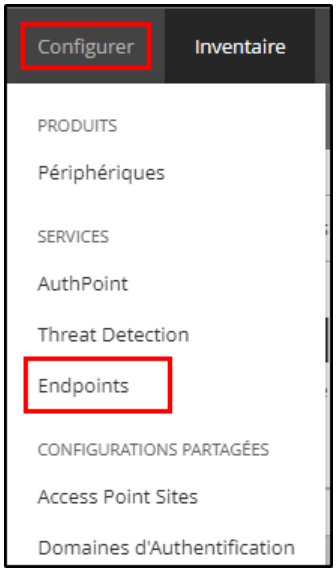
Préparation à l'installation :

Comme précisé plus haut, avant d'installer les EPDR sur les postes et serveurs, il faut préparer l'arborescence et les profils.

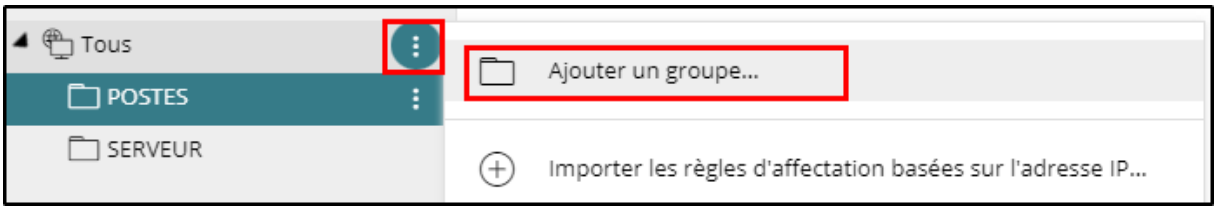
Concernant l'arborescences, vous allez avoir plusieurs possibilités qui dépendront de ce que vous souhaitez faire avec le client mais aussi de l'organisation de celui-ci.

Vous aurez plusieurs choix possibles dont celui de lier l'arborescence à l'AD. Nous n'allons pas l'aborder ici, mais plutôt utiliser des groupes.

Pour ça, tout simplement sélectionnez le client, puis allez dans « Configurer » puis « Endpoint » :



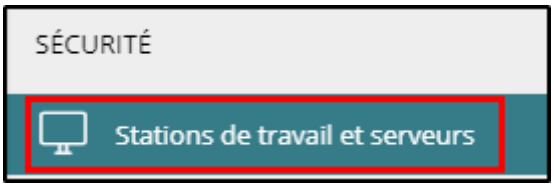
Ensuite dans l'onglet « Ordinateurs » vous avez un groupe par défaut « Tous », sous ce groupe vous allez pouvoir créer l'arborescence que vous souhaitez, pour ça cliquez sur les 3 petits points, puis « Ajouter un groupe » :



Maintenant que l'arborescence est en place, il va falloir modifier quelques profils par défaut. Dirigez-vous dans « Configuration » puis dans « Paramètres par ordinateur ». Ici vous allez pouvoir définir le mot de passe de configuration du logiciel. Pour ça copiez le profil par défaut pour en créer un nouveau et nommez-le comme vous le souhaitez.

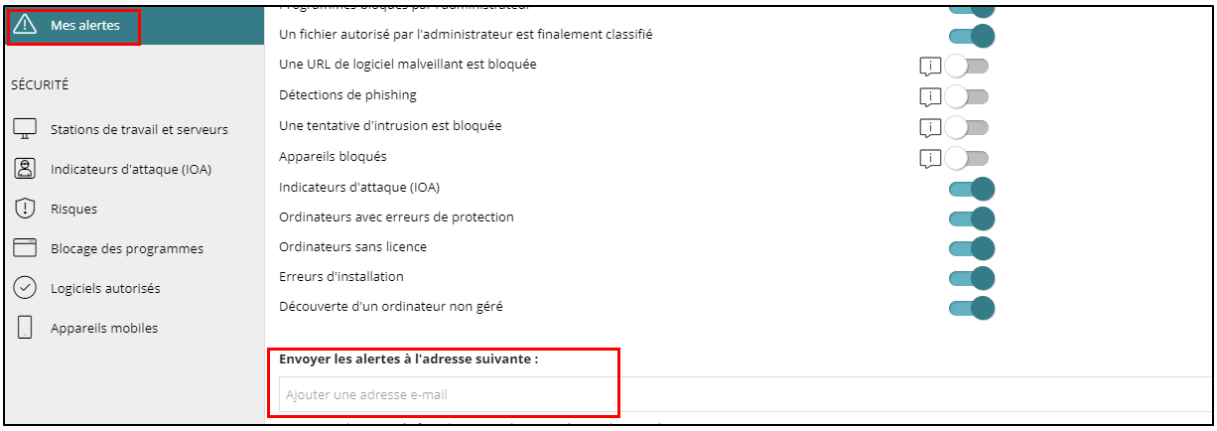
L’assisant va vous proposer de choisir un mot de passe, mettez-en un de 15 caractères avec Maj, Min, Caractère spécial et chiffre (pensez à le noter dans le DT du client). Choisissez le groupe que vous souhaitez, vous pouvez choisir un groupe spécifique ou alors « Tous », qui aura pour effet de se déployer sur tous les postes des groupes (sauf si vous avez spécifier une configuration sur un de ses groupes).

On va passer sur la partie protection, rendez-vous dans « Configuration » puis « Stations de travail et serveurs » dans sécurité. Copiez aussi le profil par défaut pour en créer un nouveau. Ici modifier principalement plusieurs choses (en dehors de l’attribution des rôles selon l’arborescence et la stratégie souhaitée) :



- **Général :** Vous pouvez le laisser par défaut.
- **Protection avancée :** Ici c’est un élément clé de l’EPDR. Il faut pour l’installation passer en mode **Audit** (mode qui ne bloque rien) puis après passer en mode **Hardening** (mode d’apprentissage à laisser 2 semaines minimum et 4 grand maximum). A la fin de cette période de plusieurs semaines, il faut passer en mode **Lock** afin de finaliser l’installation de l’EPDR.
- **Antivirus :** Vous pouvez laisser la configuration par défaut.
- **Firewall :** Il est désactivé par défaut, vous pouvez simplement cocher la case « Activer le firewall ».
- **Contrôle des appareils (Windows uniquement) :** Il est désactivé par défaut, vous pouvez l’activer si le client le demande, sinon laissez désactiver.
- **Contrôle de l’accès au Web :** C’est aussi désactivé par défaut, à voir avec le client s’il souhaite l’activer ou non.

Pour information, par défaut les alertes sont envoyées au compte qui a créé le compte client, vous pouvez supprimer le mail ou en choisir une autre dans l'onglet « Mes alertes » dans le panneau de configuration EPDR :



Voilà, avec ça vous avez configurer un EPDR de façon basique et sans module particulier. Si c'est le cas, la stratégie reste la même, il faut le préparer en amont et bien définir les rôles avant installation.

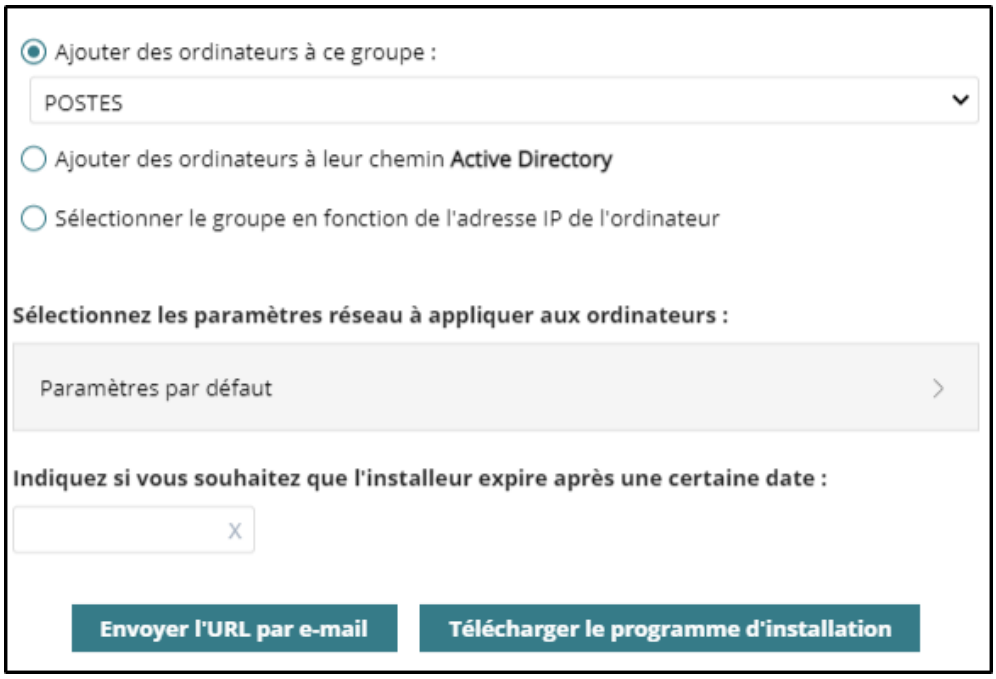
Installation :

Voilà, avec ça vous Comme pour tout logiciel, vous avez la possibilité d'installer l'EPDR de plusieurs façons, soit en envoyant un lien à l'utilisateur, soit via GPO, soit via une image Windows, soit directement via le PC avec le package MSI.

Ici nous allons simplement montrer comment télécharger le package MSI. Pour ça rendez vous dans le groupe sur lequel vous souhaitez ajouter le poste et cliquez simplement sur « Ajouter un ordinateur » :

Ensuite il vous proposera de choisir la plateforme d'installation (l'installation sur les SE autre que Windows sont tout aussi facile que sur celui-ci).

Une fois la plateforme sélectionnée, vous pourrez changer de groupe, changer les paramètres réseaux à appliquer et choisir entre envoyer le mail ou directement télécharger le MSI :



Pour la suite c'est à vous de voir comment procéder à l'installation, vous pouvez faire une GPO via ce MSI laisser l'utilisateur installer lui-même son logiciel ou alors aller l'installer manuellement ou directement prendre la main sur le poste du client.

Une fois installé, passez en mode Hardening et notez-vous de passer en mode Lock quelques semaines plus tard (pas plus de 4 semaines).

C'est terminé pour l'installation et la mini configuration de l'EPDR.