Utilisateur	Application
Mise en place dispositif	
-Association filaire entre le modem et le dispositif où l'application va être lancée -Exécution de l'application avec les droits administrateurs	-vérification configuration réseau : adresse bien obtenue dans le LAN, modem configurable par l'utilisateur,... -lecture des fichiers de configuration déjà présents : quels modules doivent être chargés et mis en file d'attente et avec quels paramètres (fréquence, ...) -vérification des dépendances à respecter pour ces modules (présence d'un chipset compatible pour sniffing wifi,...)
Paramétrage manuel	
-choix d'un dump précédent à charger (fichier xml) ou lancer une nouvelle session vierge à configurer -possibilité de compléter/créer des équipements dans l'application correspondant à ceux réellement dans le réseau domestique (instances virtuelles) pour pallier à ce que l'application ne trouve/déduit pas -communication facultative des identifiants/mdp (du modem, wifi, équipements), du mail à notifier	-parsing du fichier de sauvegarde, interface pour modifier le contenu chargé en rectifiant les caractéristiques et informations relatifs à chaque équipement (instances virtuelles) : >type/fonction >fabricant et modèle >version firmware >adresses MAC et dernière IP >services/ports ouverts >protocoles utilisés >(récapitulatif des événements/alertes de sécurité concernant l'équipement) -chiffrement et stockage des identifiants
Configuration de la routine de surveillance	
-sélection de quels modules doivent être utilisés, classés en deux catégories : actifs ou passifs - configuration de la fréquence d'exécution de chaque module actif -ajustement de paramètres spécifiques à chaque module	- instanciation de l'ensemble des modules qui seront exécutés dans la routine définie par l'utilisateur avec les paramètres donnés - association d'un timer à chaque module étant catégorisé actif et d'un état booléen "en cours" aux modules passifs - attente du lancement de la routine par l'utilisateur, marque le lancement des timer et la mise en route des modules passifs

Routine : modules actifs

- les modules dont l'exécution a été planifiée dans la routine peuvent être présentés comme une file ordonnée par le temps restant avant déclenchement

- des modules peuvent être rajoutés dynamiquement dans cette file, suspendus pour la routine courante ou supprimés

-possibilité de lancer l'exécution d'un module actif indépendamment de la routine courante

- réception d'un mail de feedback si un danger est repéré

- modules qui vont interagir directement avec les équipements du réseau pour déceler un danger

- scripts automatisés lancés sur des cibles arbitraires encore non recensées par l'application ou en utilisant l'information déjà récoltées sur les équipements

- utilisation de l'output des scripts derrière les modules pour rectifier/améliorer les instances virtuelles des équipements

Routine : modules passifs

- possibilité d'ajouter / supprimer / suspendre des modules passifs dans la routine en cours

- réception d'un mail de feedback si un danger est repéré

- modules qui basent leur détection des menaces sur une écoute passive de ce que le dispositif peut capter, aucune confrontation directe avec les autres équipements du réseau

- les modules sont lancés quand la routine démarre et restent fonctionnels tout du long: ensemble de modules passifs en cours ou suspendus par action de l'utilisateur

- sous forme de processus tournant en arrière plan, surveillant une certaine ressource pouvant être un indicateur/vecteur de menace

- utilisation de l'information capturée pour rectifier/améliorer les instances virtuelles des équipements

Informations récoltées : instances virtuelles

- une instance représente un équipement détecté dans le réseau domestique et regroupe toutes les informations connues (champs) qui lui sont propres

- une instance peut être créée et ses champs complétés soit par l'utilisateur lui même soit depuis un module qui permet d'acquérir de l'information à son propos

- maintient une liste des équipements dont on minimise les doublons (principe input utilisateur prime sur détection automatique), totalement modifiable par l'utilisateur

- champs de chaque instance indexé par un nom fixe, plusieurs optionnels

- état associé à chaque équipement en fonction de son activité sur le réseau, logs de détection de menace relatives à l'équipement