CRUSOE CIDS

http://www.crusoe-researches.com

email: contact@crusoe-researches.com

Table des Matières

La société

- Société française de services et d'édition de logiciels dans le domaine de la sécurité informatique.
- Constituée autour d'un groupe d'experts de la sécurité, du développement et des systèmes d'informations.
- Décline une gamme de services basée sur une solution complète de détection d'intrusion et d'analyse d'impacts nommée CRUSOE CIDS propriété intégrale de CRUSOE Researches.
- Projet démarré en 2002, suite à l'analyse des besoins métier spécifiques à la sécurité informatique et à l'inexistence de solution industrielle satisfaisante.
- Continue à accroître son expertise dans tous les domaines de la sécurité.

Pourquoi CRUSOE CIDS ?

- Grande diversité des détections d'intrusion sur le marché (NIDS, IPS, etc...)
- Dispersion et éloignement des sources d'informations au sein d'une même entreprise.
- Redondance et similitude des événements.

  ⇨**Standardisation, agrégation et centralisation des logs.**
- Grand nombre d'événements remontés par les détections d'intrusion.
- Difficultés à déterminer la pertinence ou l'impact d'un événement.

  ⇨ **Automatisation des traitements.**

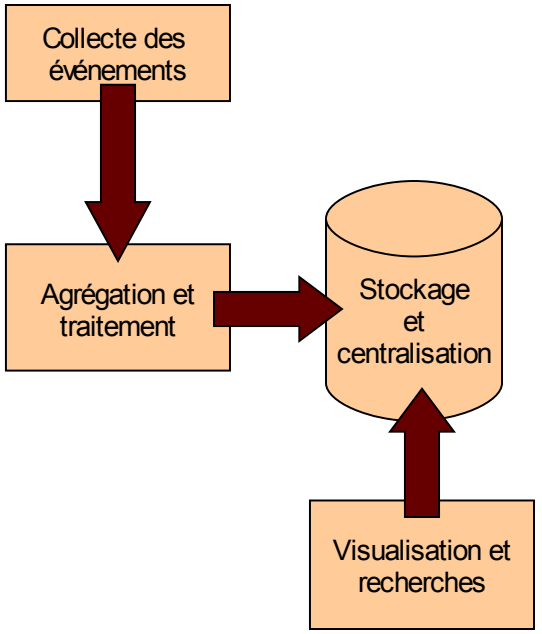
  ⇨ **Corrélation des événements avec l'analyse automatique du trafic réseau, pour permettre un diagnostic.**
- Besoins de réactivité face à l'apparition de nouvelles attaques.
- Richesse et diversité du monde open-source en terme d'outils par rapport aux produits classiques.

  ⇨**Langage de scripting permettant l'ajout de traitement d'attaque et l'emploi de n'importe quel outil.**

Les principes

CRUSOE CIDS est constitué de 3 niveaux distincts :

- Un niveau de collecte des informations
- Un niveau de traitement des informations
- Un niveau de visualisation des informations



Le niveau de collecte

Il est opéré à l'aide de différents constituants :

- Détection d'intrusion à l'aide de NIDS open-source reconnus dans le domaine (sans limite du nombre d'outils intégrés).
  - Snort
  - Prelude
  - Firestorm
  - Bro
- Enregistrement du trafic réseau simultanément à la détection, à l'aide d'outils CRUSOE Researches basés sur le format standard tcpdump.
- Collecte des événements format syslog remontés par les NIDS ainsi que la préparation de l'agrégation de ceux-ci par l'outil logscan de CRUSOE Researches.
- Collecte des événements de Firewall tel que iptables

Le niveau de traitement

Il constitue le cœur du CRUSOE CIDS et permet :

- Agrégation des événements redondants et stockage en base de données.
- Traitement automatique visant à la détermination de l'impact des événements. Corrélation des réponses réelles des serveurs à partir du trafic enregistré.
- Détermination du scoring à partir de la valeur CVSS et de la topologie pour déterminer l'importance effective.
- Enrichissement à partir des données externes pour affiner les diagnostics (whois, country, etc…).
- Corrélation des événements provenant de sources différentes (firewalls/nids) permettant un calcul dynamique de leur sévérité.
- Détection de comportement par analyse des anomalies dans les logs.

Le niveau de visualisation

Il est opéré à l'aide d'une interface web sécurisée permettant :

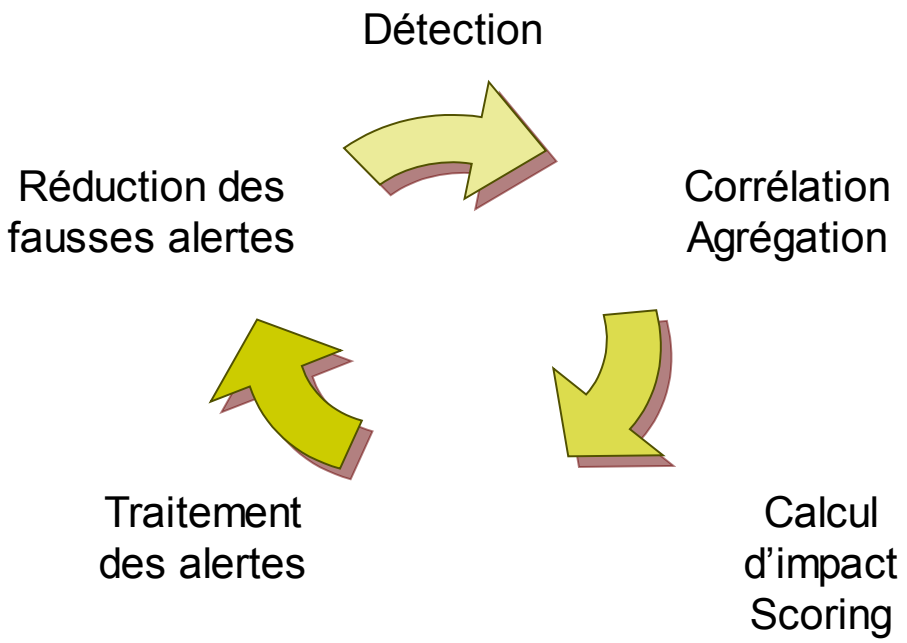
- la consultation en temps réel des événements agrégés avec les analyses d'impacts correspondantes.
- la visualisation des événements avec leur provenance (whois/country)
- la consultation des statistiques réseau à l'aide de l'outil « open-source » NTOP. Il permet de contrôler les surcharges ou sous-charges anormales.
- d'accéder à des outils de recherches croisées multicritères pour repérer des comportements particuliers.
- la consultation des statistiques de l'état du système.

La gestion des règles de détection

La mise à jour des règles de détection d'intrusion est obligatoire pour permettre de détecter les nouvelles attaques et fait partie des services proposés par CRUSOE Researches :

- Le nombre de règles SNORT disponibles publiquement : 3581.
  (depuis la version 2.3.3 de snort)
- Le nombre de règles SNORT appartenant à « Community » : 178 (!).
  (« Community » est le mode de licence publique SNORT).
- Le nombre de règles SNORT mise à jour par CRUSOE Researches : 2000.
  (Nous travaillons depuis plus de deux ans à optimiser celles-ci).
- Le nombre de nouvelles règles SNORT créées par CRUSOE Researches : 846.
  (réservées à nos clients).

Cycle d'amélioration de la détection



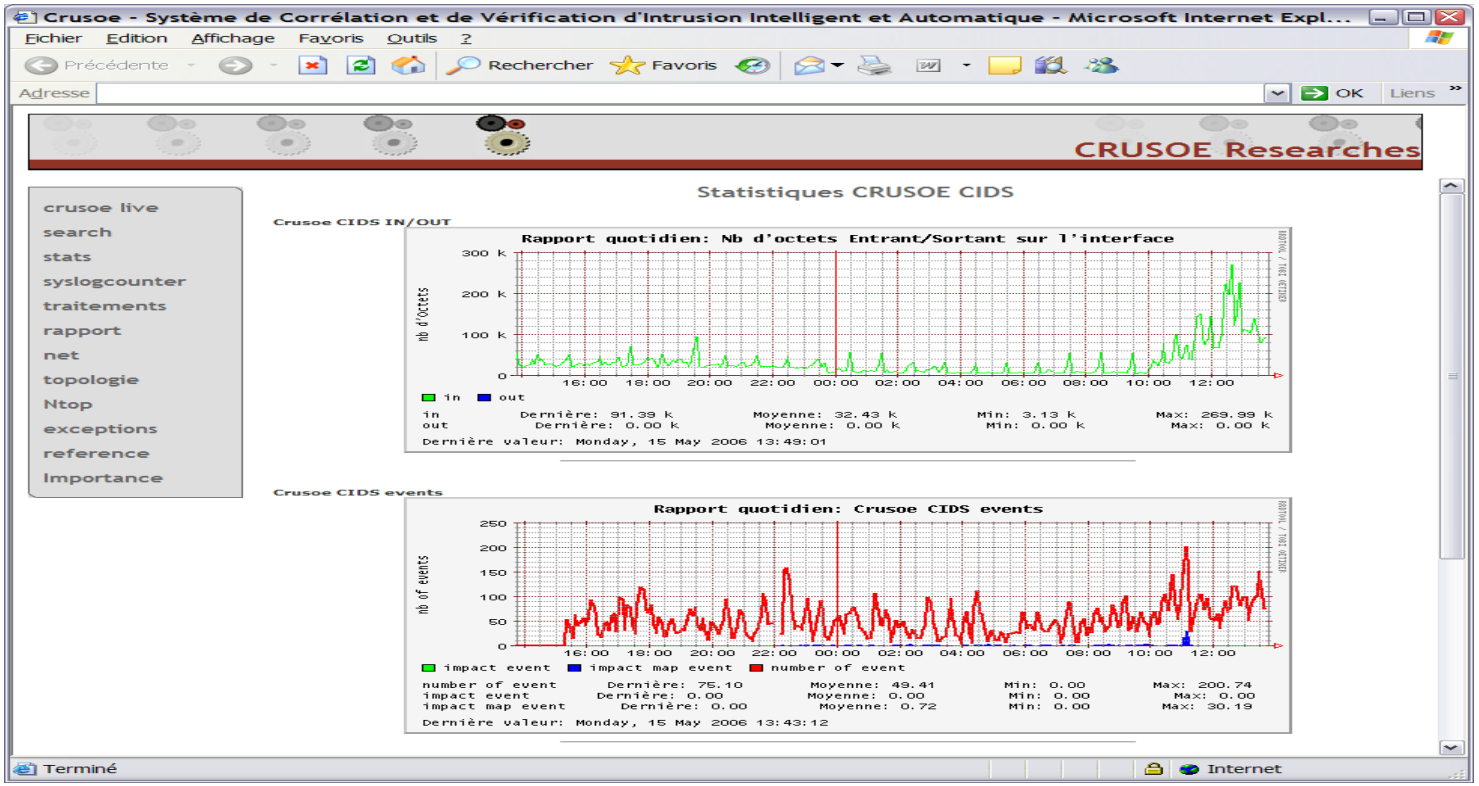
- une alarme est détectée, une agrégation et une corrélation est possible.
- le calcul de l'impact ainsi que le scoring permettent d'évaluer la gravité effective de l'alarme.
- les alarmes importantes sont analysées pour réduire leur nombre en modifiant les règles de détection par exemple.

Vulnerability Assessment

Crusoe CIDS dispose d'un module permettant pour les événements de déterminer la classification selon les standards du marché

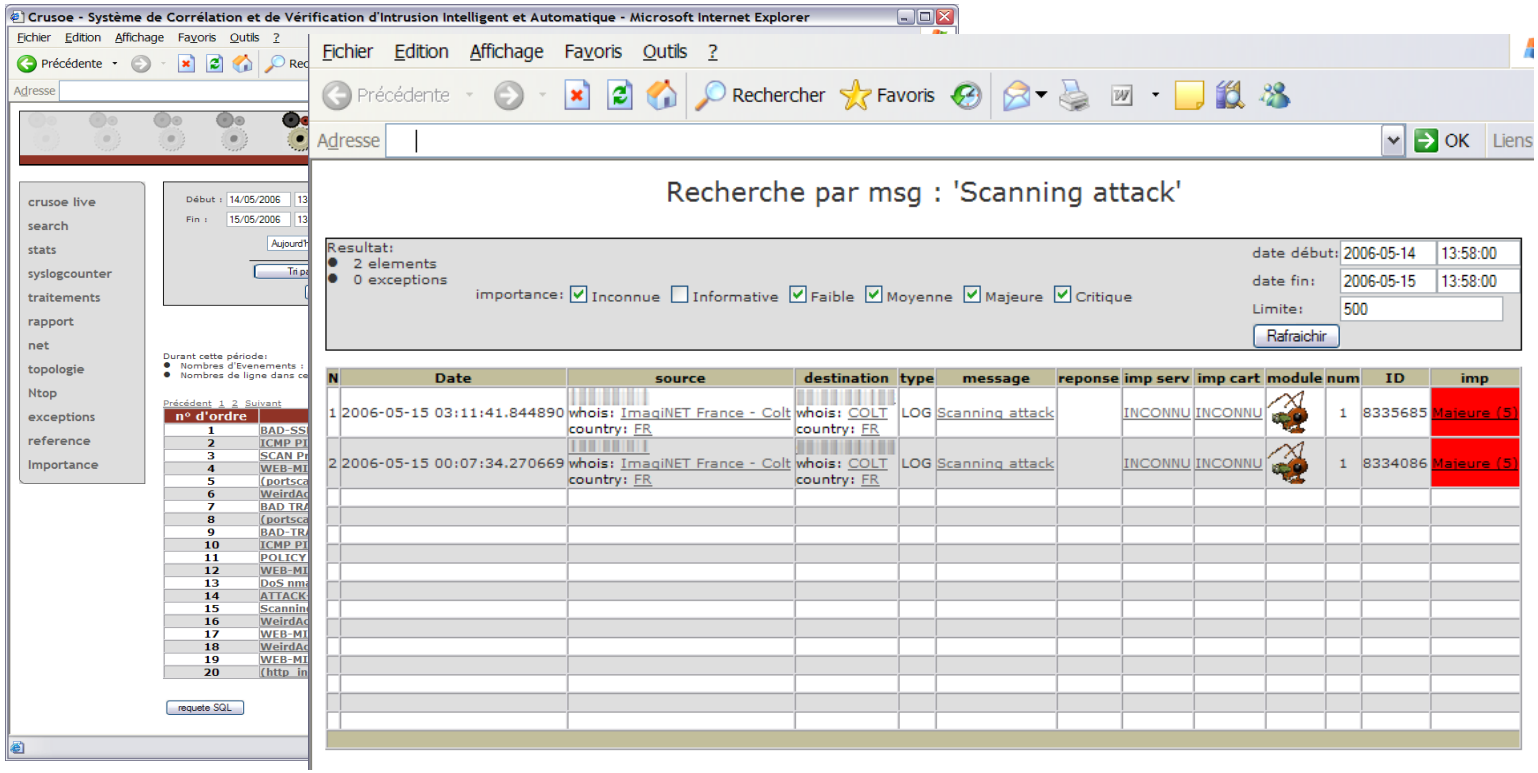
- Nessus
- ISS
- Common Vulnerabilities and Exposures (CVE)
- Osvdb
- Microsoft
- Ciac
- Oval
- Snort
- US-cert

Pour permettre une liaison avec les outils de sécurité en place au sein de la société !



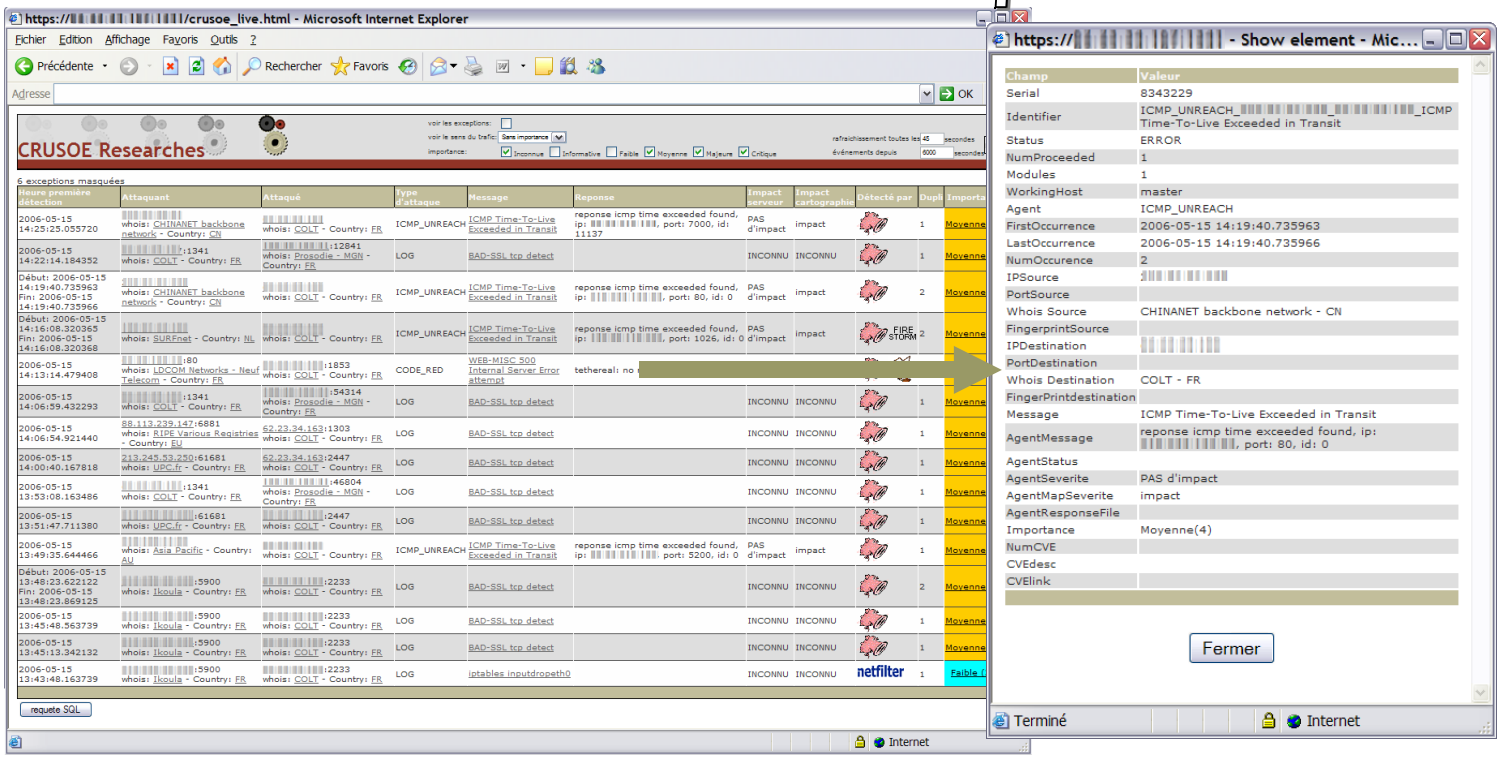
La page d'accueil permet d'accéder rapidement à l'état du système.

CRUSOE Researches



La recherche permet de naviguer simplement parmi les faits marquants de la journée.

Les interfaces : le temps réel

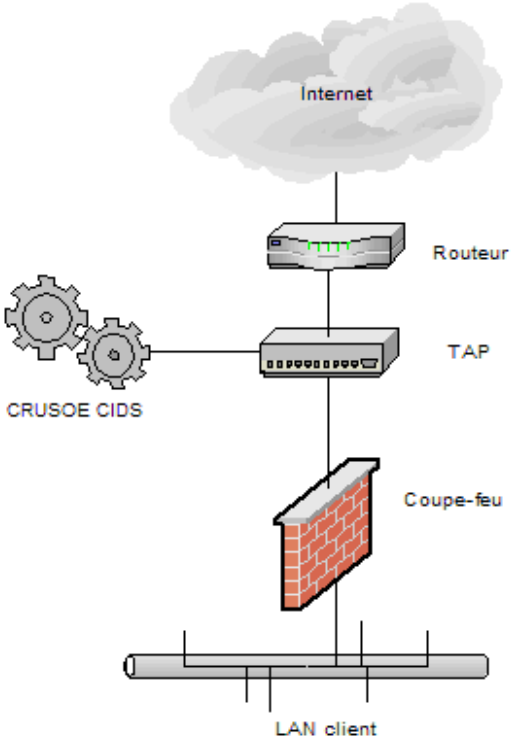


Permet de suivre les événements au fil de l'eau ainsi que le détail pour chacun d'eux.

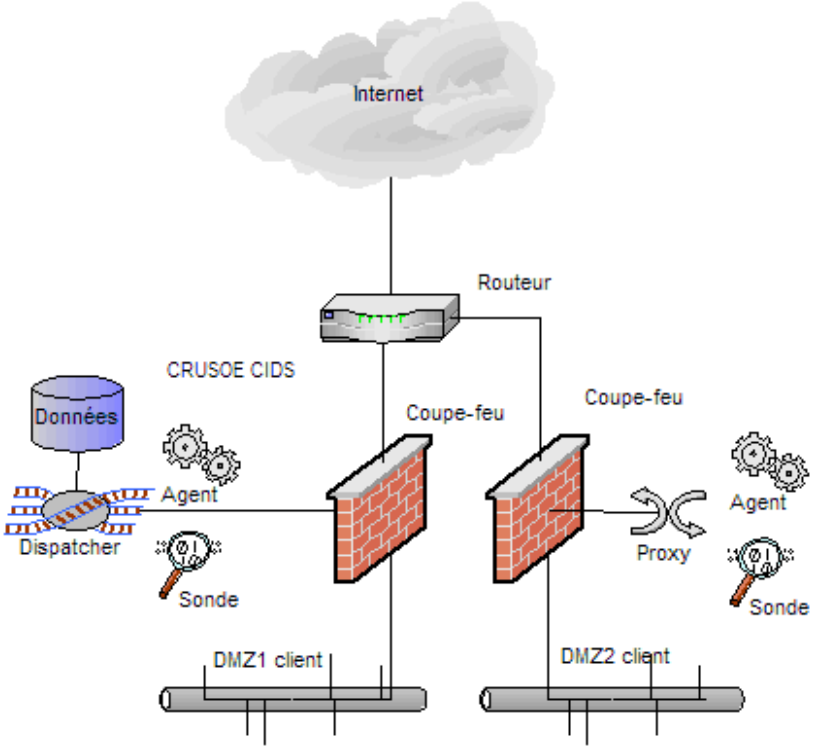
L'architecture

CRUSOE CIDS s'adapte à différents type d 'architecture.

ARCHITECTURE SIMPLE



ARCHITECTURE DISTRIBUEE



Les Atouts

- Modularité
  - Ajout possible de nouvelles fonctionnalités ou d'outils à chacun des trois niveaux, sans limite et sans nécessité de licences supplémentaires.
  - Utilisation d'un langage de programmation commun pour les niveaux de collecte et de traitement, permettant une parfaite cohérence et intégration.
  - Utilisation possible de différents SGBD (postgresql, oracle, etc…) pour le stockage et pour l'enrichissement : pas de redondance de l'information nécessaire.
- Autonomie
  - Les constituants et les métriques critiques sont contrôlés automatiquement afin de garantir une utilisation continue et des performances optimales : surveillances process, espace disque, purges des données, etc...
  - Tous les éléments sont disponibles pour l'administrateur à des fins d'analyse, de diagnostic et de preuves légales.
- Sécurité
  - Utilisation d'un OS (FreeBSD) réputé pour la sécurité et d'une installation épurée avec des modifications de paramétrage et cloisonnement des process.
  - Possibilités de fonctionnement en architecture distribuée avec flux cryptés.

Les Atouts (suite)

- Efficacité/Rentabilité
  - Solution complète de la détection réseau aux traitements par l'analyste sécurité. Améliore l'efficacité en élevant la qualité des traitements tout en réduisant les coûts humains.
  - Réduction des temps de traitements et des délais de diagnostic d'impact.
  - Possibilité d'utiliser des outils « domaine public » pour réduire davantage les coûts.

Les prestations

CRUSOE Researches propose les services suivants :

- L'installation, la mise à jour et le support de CRUSOE CIDS et de ses constituants (OS, NIDS, outils, SGBD).
- L'analyse et le traitement complets des événements de sécurité.
- L'alerte par mail ou SMS.
- La location « d'appliances » adaptés aux besoins des clients.
- L'analyse des architectures réseau ainsi que l'établissement de recommandations sur celles-ci.

Azwalaro

CRUSOE Researches propose un nouvel outil NIDS :

- Projet Open Source (licence GPL)
- Basé sur la librairie Ethereal (maintenant Wireshark)
- Nouveau format de règles de détection
- Réduction du nombre de fausses alertes (pbs d'uricontent avec snort !)
- Utilisation des « dissecteurs » propres à Ethereal permettant une détection sur beaucoup de protocoles (netbios/ssl/smtp/ftp/dns/…..)
- Projet en début de développement !

⇒http://www.Crusoe-Researches.com/azwalaro/

email: azwalaro@Crusoe-Researches.com

BONUS

Questions ?

Merci

http://www.crusoe-researches.com

email: contact@crusoe-researches.com