

VIGIL@NCE

VEILLE SUR LES VULNÉRABILITÉS



Une veille sur les vulnérabilités ...

Vigil@nce se veut directement et quotidiennement utilisable par vos services, afin de maintenir en permanence la sécurité de vos systèmes.

Cette veille se compose de quatre volets principaux :

- 1** Mise à disposition des informations (vulnérabilités et parades) sur un serveur web
- 2** Envoi de messages d'alerte, relatifs à la découverte de vulnérabilités importantes.
- 3** Envoi de messages quotidiens de synthèse.
- 4** Envoi de messages hebdomadaires recensant les parades.

Les travaux de l'équipe Vigil@nce s'organisent en 3 étapes :

- ☐ **Etape 1 :** Les informations brutes **sont extraites quotidiennement d'un millier de sources (web, newsgroups, mailing-lists, etc ...)** sélectionnées.
- ☐ **Etape 2 :** Les informations brutes sont analysées par une équipe d'experts dédiée à la veille technique sécurité. La sélection des informations jugées pertinentes est effectuée à partir de critères tels que la crédibilité technique d'une vulnérabilité ou d'une parade, le recoupement entre diverses sources d'information, etc.
- ☐ **Etape 3 :** Les informations jugées pertinentes lors de l'étape 2 sont classées et stockées dans une base de données où elles sont mises à disposition sous forme de fiches descriptives.

Pour être informé chaque jour ...

Les postes clients, accèdent à la page d'accueil du serveur web à l'aide d'un navigateur et s'identifient. Après avoir été authentifiés, ils émettent des requêtes vers la base de données, via une interface HTML conviviale (accès à l'ensemble de la base, recherche selon divers critères, etc.).

Disponible sous forme d'abonnement

Le coût de l'abonnement annuel à Vigil@nce est de 5 300 €HT (offre valable jusqu'au 31/12/2004).

Chaque client dispose de 3 identifiants (login et mot de passe) mis à jour trimestriellement qui permettent d'accéder simultanément à la veille et peuvent être mis à la disposition d'au maximum 10 utilisateurs.

Le périmètre de la veille peut être restreint ou étendu en fonction des besoins réels de l'abonné.

Extrait des composants suivis :

Protocoles :

- ☐ IP, TCP, UDP, ICMP
- ☐ HTTP, SMTP, FTP, DNS, IMAP, POP, SNMP

Firewalls :

- ☐ Firewall-1
- ☐ PIX

Navigation/messagerie :

- ☐ Internet Explorer
- ☐ Lotus Notes
- ☐ Netscape
- ☐ Outlook
- ☐ Outlook Express

Systèmes d'exploitation :

- ☐ AIX
- ☐ Tru64 UNIX
- ☐ FreeBSD
- ☐ HP-UX
- ☐ IRIX
- ☐ Linux
- ☐ Novell Netware
- ☐ Solaris
- ☐ Windows

Routeurs :

- ☐ Cisco
- ☐ 3Com

Serveurs :

- ☐ Apache
- ☐ Bind
- ☐ Exchange
- ☐ IIS
- ☐ Lotus Domino
- ☐ Sun ONE
- ☐ Sendmail
- ☐ Oracle

Et de nombreux autres ...

Contacts :

Laurent Constantin,
Responsable technique,
laurent.constantin@aql.fr

Hervé Gourlaouen,
Directeur commercial,
herve.gourlaouen@aql.fr

<http://vigilance.aql.fr/>