Atelier Sécurité / OSSIR

eEye® Digital Security

Présentation Produits eEye

SecureIIS

Retina

elorrain@eeye.com & broussel@eeye.com

Sommaire

- **Qui sommes nous ?**
- **SecurelIS – Protection Web**
- **Retina – Scanner de Sécurité**
- **Questions**

eEye® Digital Security

Curriculum Vitae

- **Créé en 1998**
- **Siège aux USA (CA) / Siège international à Genève**
- **Filiales à Londres et Paris**
  - Clients dans plus de 40 pays
  - Partenaires dans plus de 20 pays

- **Mission**
  - Développer des **logiciels** innovants dédiés à la **sécurité proactive**, destinés aux administrateurs réseaux et consultants. Ces produits complètent des outils comme les firewalls, les systèmes de détection d'intrusion ou les scanners de virus, pour obtenir une sécurité la plus complète possible.

- **Focus sur les vulnérabilités**
  - Le développement des produits eEye Digital Security repose sur la solide expérience de notre R&D. **eEye Digital Security** est reconnu comme étant **un des leaders dans la détection & évaluation de vulnérabilités**. (Découverte de la vulnérabilité utilisé par Code Red et de 90% des vulnérabilités de Microsoft IIS).

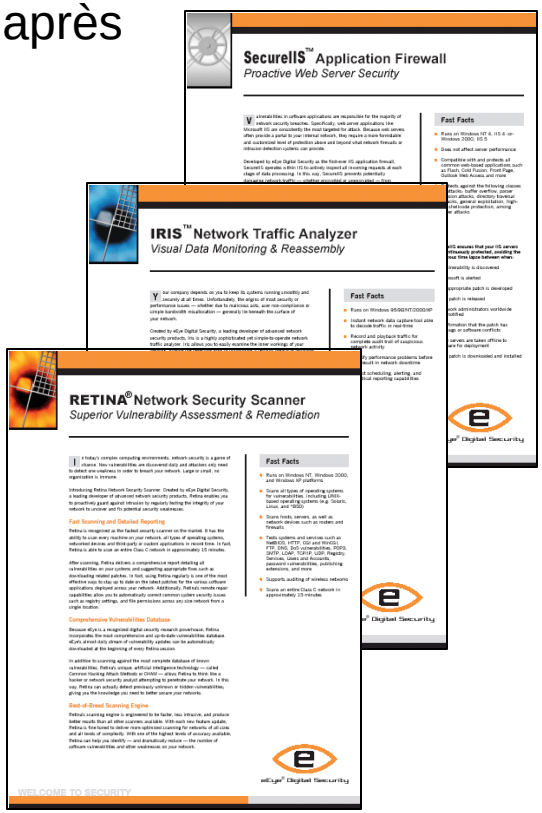
eEye® Digital Security

Stratégie Produits

- **Produits dédiés à la sécurité proactive**
  - Se protéger AVANT l'attaque – non pas pendant ou après
  - CHAM (Common Hacking Attack Methods)

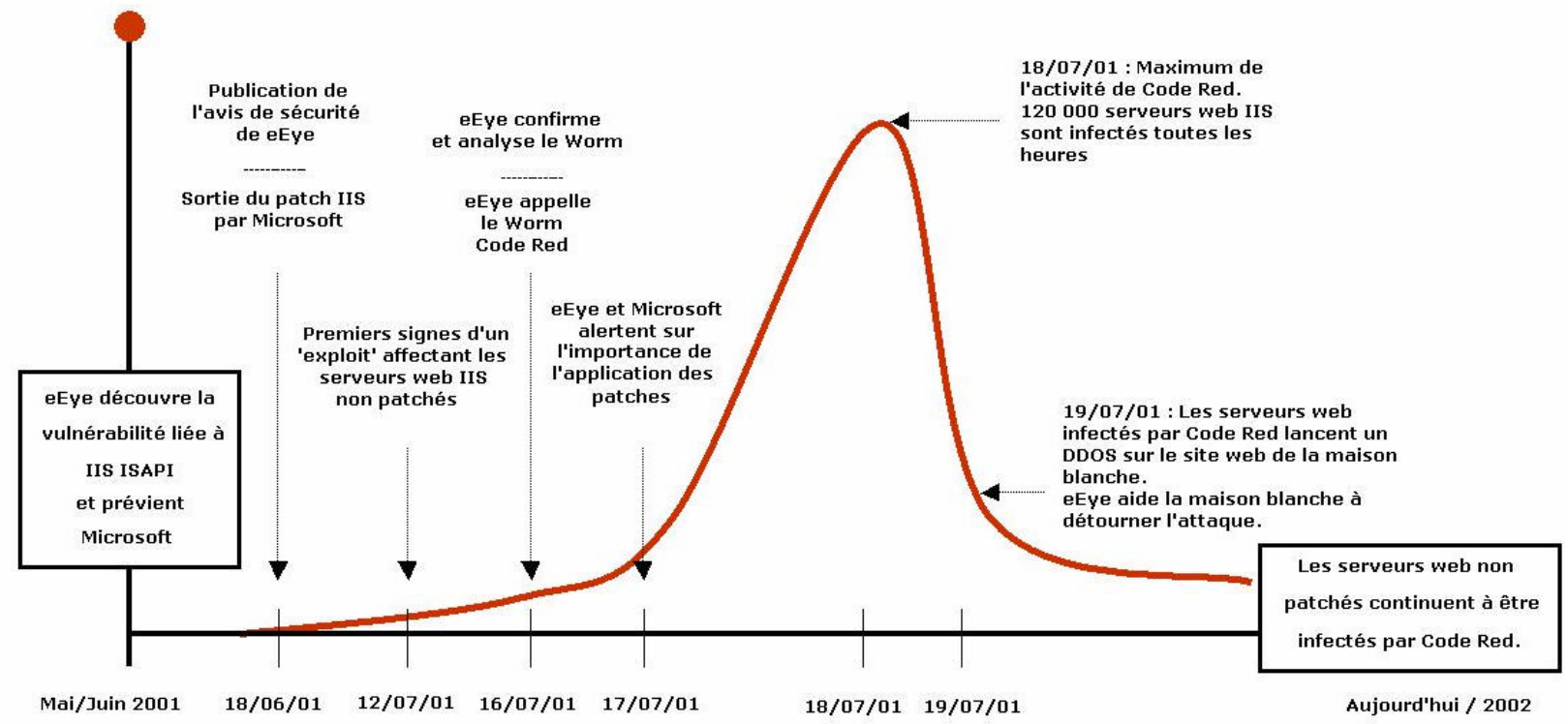
- **Conçus pour compléter les solutions existantes**
  - Firewalls
  - Intrusion Detection Systems (IDS)
  - Virus Scanners

- **Objectif : Simplicité**
  - Facile à installer, à mettre à jour, à utiliser
  - Fonctions de reporting personnalisable
  - Facilité pour mesurer le ROI (Time & Security)



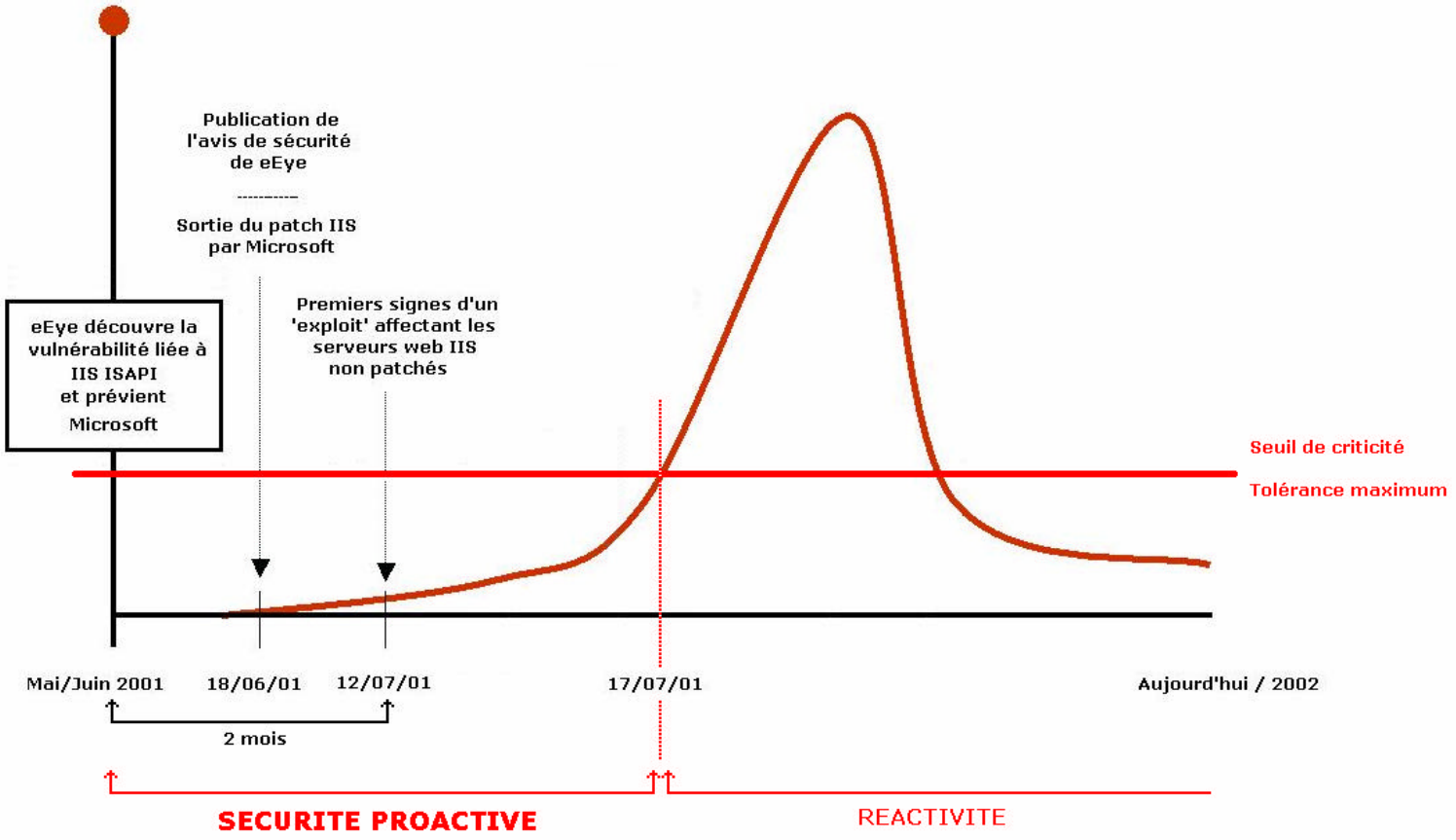
eEye® Digital Security

Exemple : Code Red Worm



eEye ® Digital Security

Approche Proactive de la Sécurité



eEye® Digital Security

Offre Produits

- **RETINA® Network Security Scanner**
  Détection, évaluation et correction des vulnérabilités
  - Le plus Rapide et le plus Complet des Scanners
    (**Network World February 2002**)

- **SecureIIS™ Web Server Protection**
  La sécurité proactive de vos serveurs Web
  - Firewall Applicatif pour Microsoft IIS

- **IRIS™ Network Traffic Analyzer**
  Surveillance et reconstitution visuelle du trafic résea
  - Enregistre les Données transitant sur le Réseau et les restitue en Différé ou en Temps Réel
  - Met en évidence les Infractions de Sécurité

eEye® Digital Security

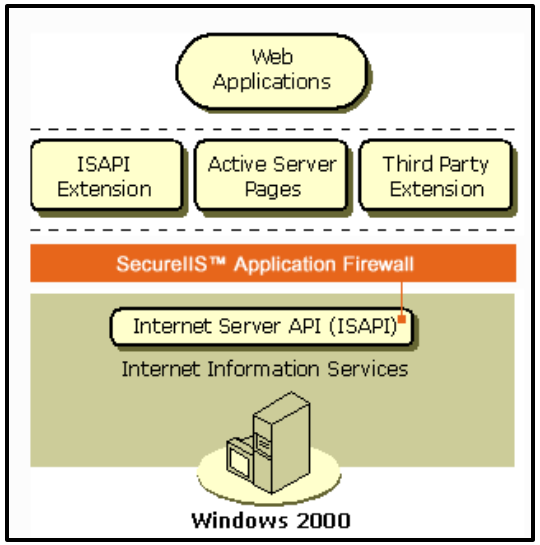
SecureIIS™ Protection Web

eEye® Digital Security

SecureIIS : Points clés

- **Le premier Firewall applicatif dédié à IIS**
- **Le seul produit intégré à MS IIS en tant que filtre ISAPI qui protège le Web Server contre des classes entières d'attaques**

- **Gestion centralisée des règles**
- **Archivage des requêtes rejetées.**
- **Paramétrage global & dynamique**
- **Statistiques temps réel**
- **Protection non intrusive**
- **Protection des applications**
- **Protection des sessions SSL**
- **Exportation des logs**
- **Compatible avec les applications Web (Outlook Web Access, Front Page, …)**
- **Monitoring du système de fichiers**

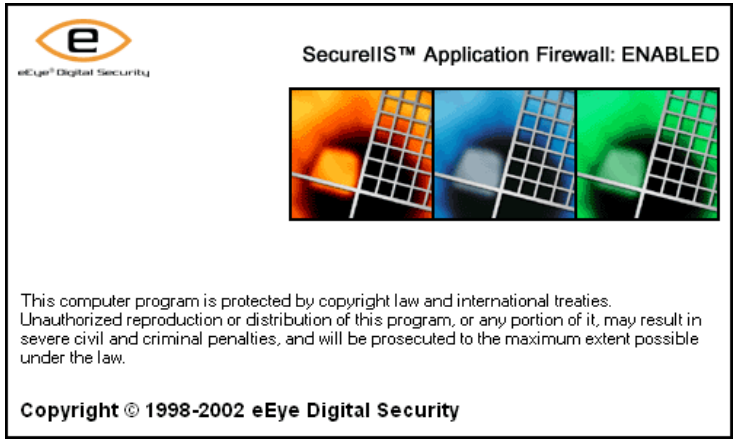


eEye® Digital Security

Sécurité Proactive

SecureIIS protège les Serveurs Web contre différents types d'attaques :

- **Dépassement de buffer**
- **Sortie du répertoire racine**
- **Exploits**
- **Protection contre les Shell Codes**
- **Vérification des RFC**
- **Vulnérabilités non connues**
- **Autres attaques…**



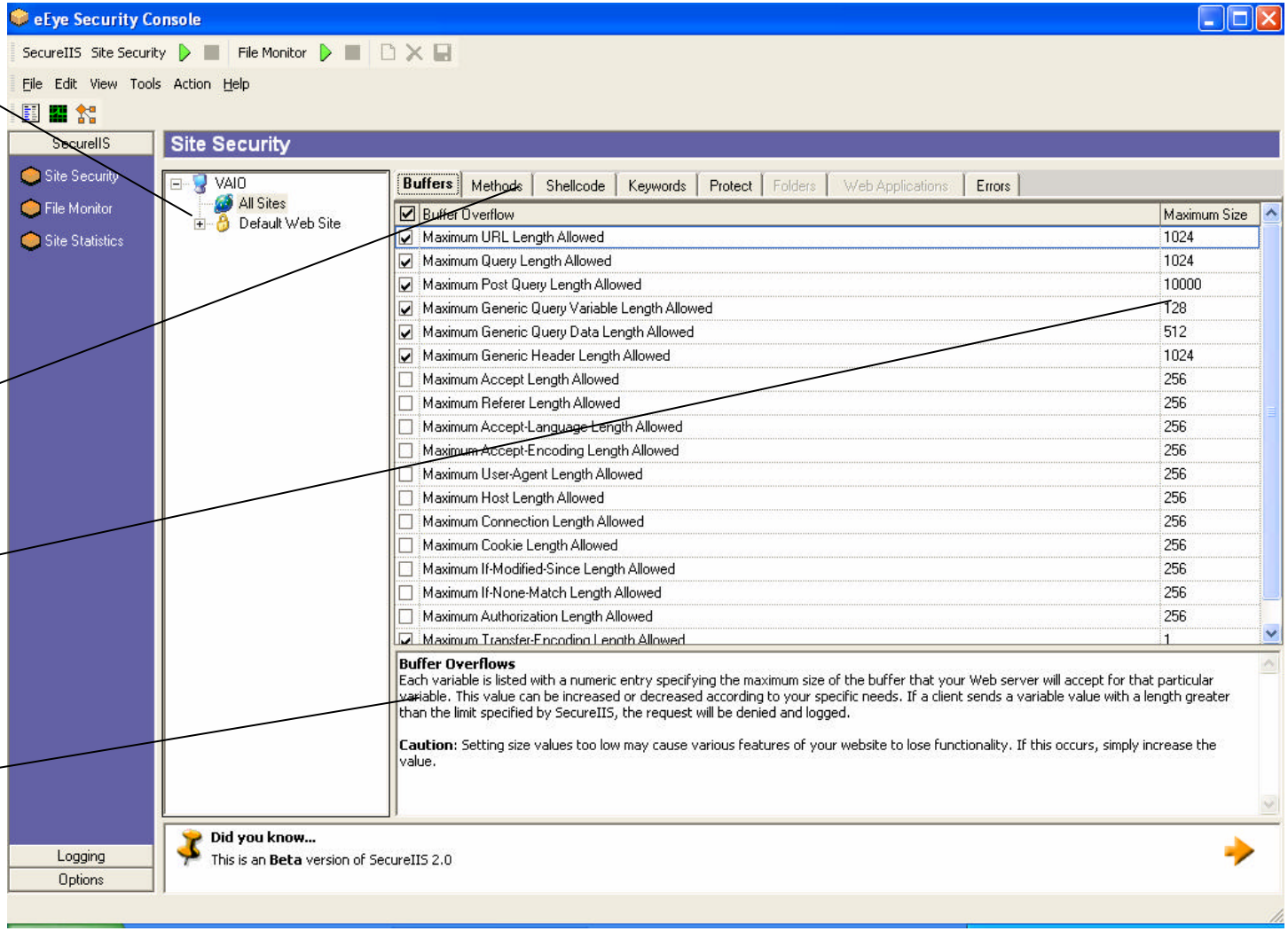
SecureIIS - Démo

Plusieurs sites Web sur un même serveur peuvent être protégés

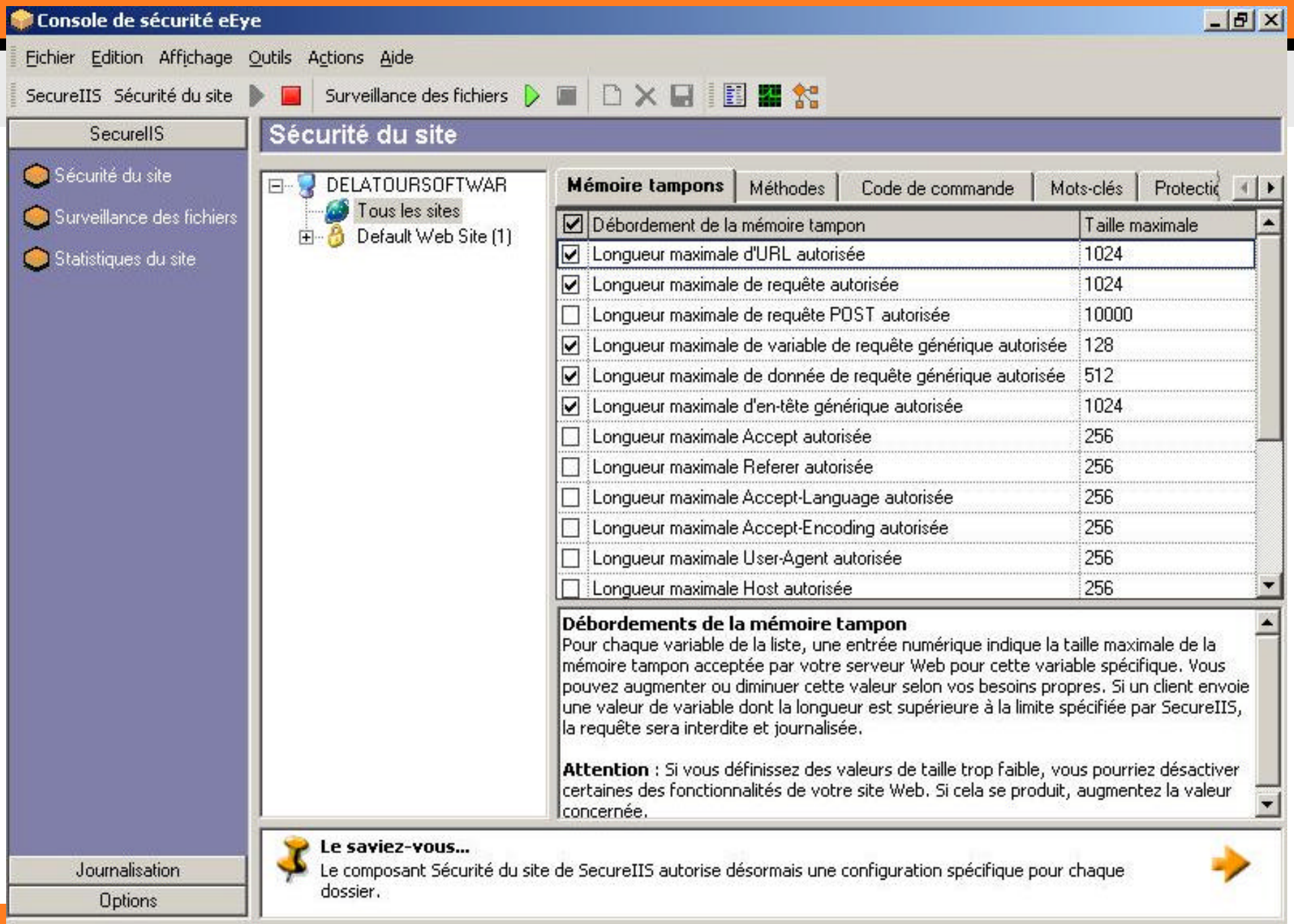
Type de classes d'attaques – Chaque onglet représente une catégorie d'attaque – chaque sous catégorie d'attaque est paramétrable

Paramètres par classe d'attaque

Chaque classe d'attaque est décrite en détails avec une aide pour la configuration



eEye® Digital Security

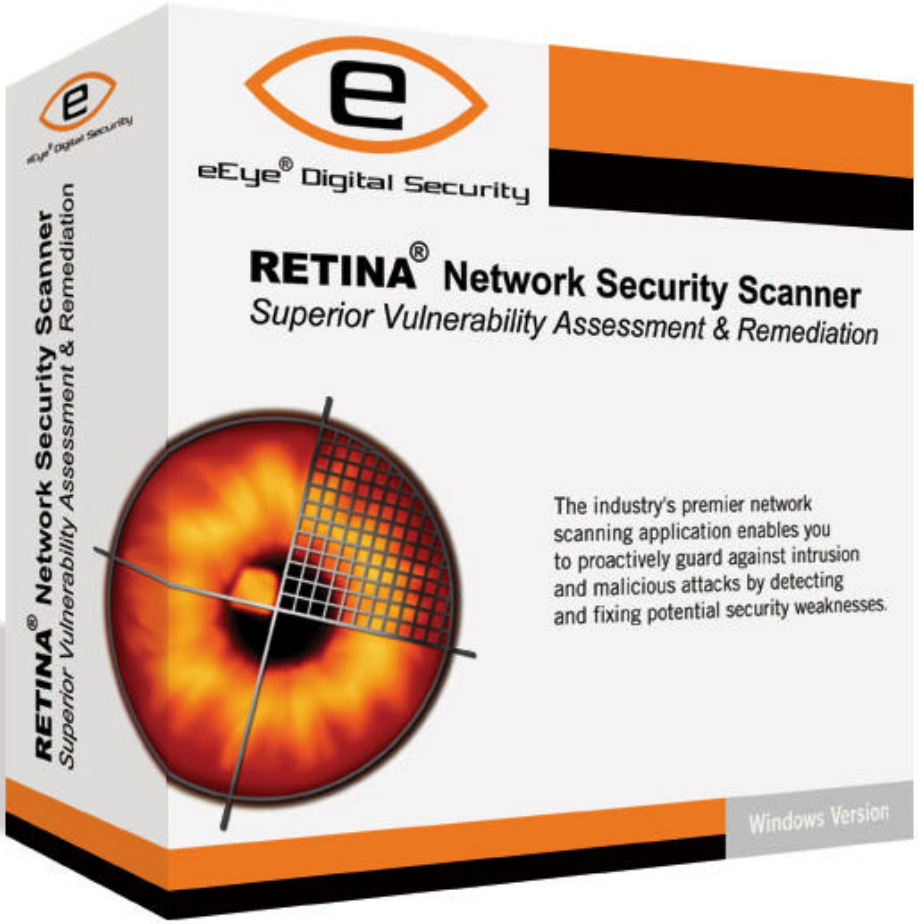

Console de sécurité eEye
Fichier Edition Affichage Outils Actions Aide
SecureIIS Sécurité du site
Surveillance des fichiers
SecureIIS
Sécurité du site
Surveillance des fichiers
Statistiques du site
Journalisation
Options
Sécurité du site
DELATOURSOFTWAR
Tous les sites
Default Web Site (1)
Mémoire tampons
Méthodes
Code de commande
Mots-clés
Protecti
Débordement de la mémoire tampon
Taille maximale
Longueur maximale d'URL autorisée 1024
Longueur maximale de requête autorisée 1024
Longueur maximale de requête POST autorisée 10000
Longueur maximale de variable de requête générique autorisée 128
Longueur maximale de donnée de requête générique autorisée 512
Longueur maximale d'en-tête générique autorisée 1024
Longueur maximale Accept autorisée 256
Longueur maximale Referer autorisée 256
Longueur maximale Accept-Language autorisée 256
Longueur maximale Accept-Encoding autorisée 256
Longueur maximale User-Agent autorisée 256
Longueur maximale Host autorisée 256
Débordements de la mémoire tampon
Pour chaque variable de la liste, une entrée numérique indique la taille maximale de la mémoire tampon acceptée par votre serveur Web pour cette variable spécifique. Vous pouvez augmenter ou diminuer cette valeur selon vos besoins propres. Si un client envoie une valeur de variable dont la longueur est supérieure à la limite spécifiée par SecureIIS, la requête sera interdite et journalisée.
Attention : Si vous définissez des valeurs de taille trop faible, vous pourriez désactiver certaines des fonctionnalités de votre site Web. Si cela se produit, augmentez la valeur concernée.
Le saviez-vous...
Le composant Sécurité du site de SecureIIS autorise désormais une configuration spécifique pour chaque dossier.

Avantages de SecureIIS

- **Gestion Plus Souple de l'Application des Patchs**
  - Protection Active & Constante des Vulnérabilités connues ou inconnues
- **Protection & Configuration Dynamique**
  - Protection par Politique & Règles (Pas de Signatures)
  - Il n'est Pas Nécessaire de Redémarrer IIS
- **Nouveau Niveau de Sécurité**
  - Pas de Modification de la Configuration de IIS
- **Gestion Centralisée**
  - Politique de Sécurité Globale
  - Centralisation des Logs (REM)

eEye® Digital Security

RETINA® Scanner de Sécurité



eEye® Digital Security

Retina: Le scanner de sécurité

- **Retina : Quelles sont les cibles des audits ?**
  - Serveurs, Stations de travail, firewalls, routeurs, etc.

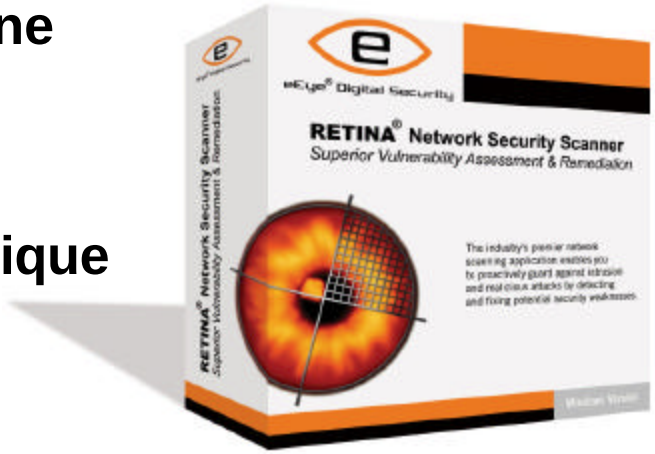
- **Retina : Audits**
  - Basé sur
    - une adresse IP
    - une plage d'adresses
    - un nom de machine

- **Retina : Résultats**
  - Evaluation du niveau de risque pour chaque vulnérabilité identifiée.
  - Description détaillée des vulnérabilités (descriptif, liens bulletins d'alerte & CVE & Bugtrack)
  - Correctif détaillé pour éradiquer les vulnérabilités (descriptif, liens patchs & correction automatique pour certaines vulnérabilités).
  - Rapport détaillé et interactif (HTML) (archivage possible des informations dans un SGBD)

eEye® Digital Security

RETINA Points clés

- #1 Scanner par Network World Magazine
- Scanner le plus rapide du marché
- Mise à jour automatique
- Correctif détaillé & Correction automatique des vulnérabilités
- Planificateur
- Architecture Ouverte & API pour personnaliser les audits
- Rapport personnalisable
- CHAM *[Common Hacking Attack Methods]*
- Détection complète des OS & Analyse des protocoles

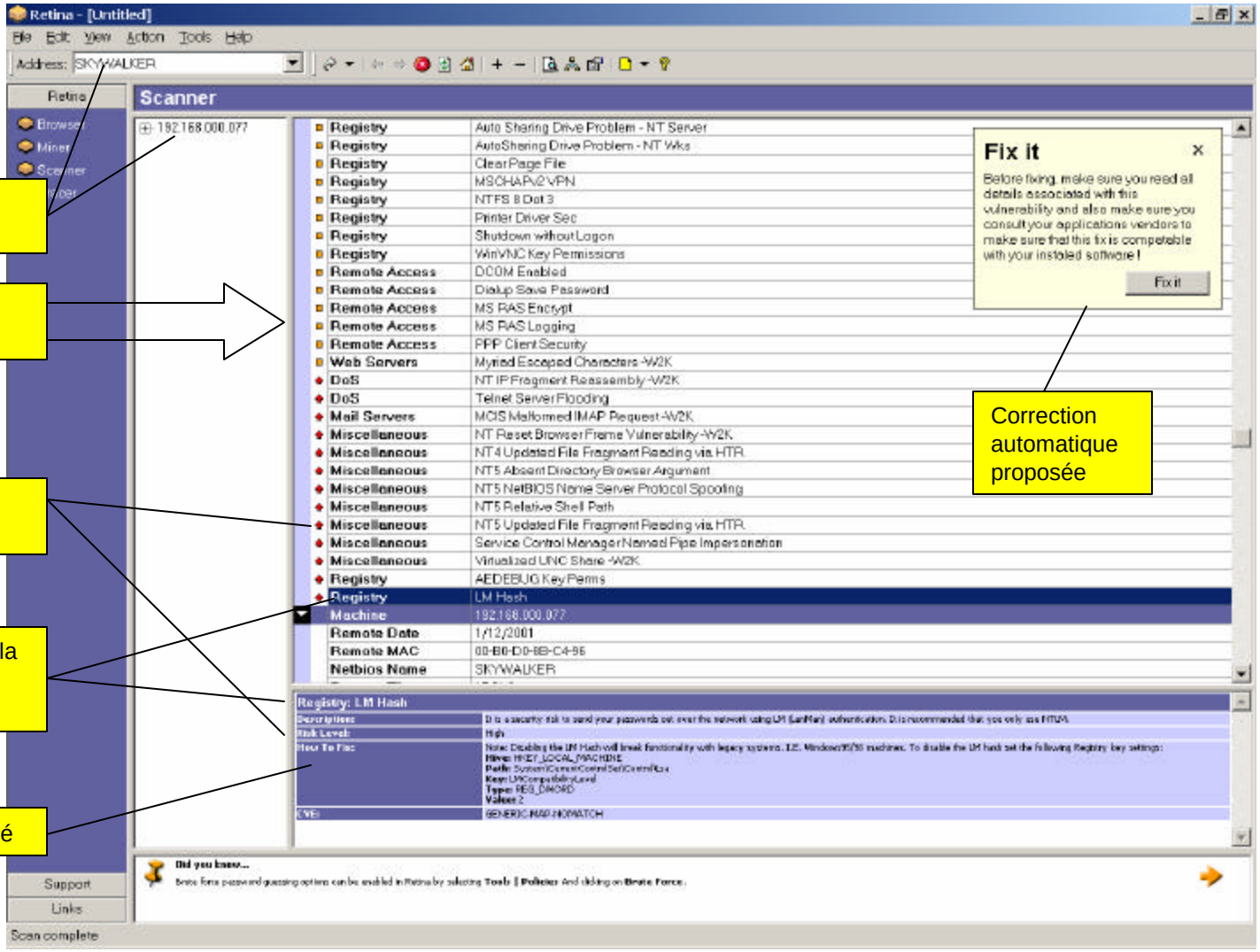


NetworkWorld BLUE RIBBON AWARD

SC MAGAZINE BEST BUY

INFORMATION SECURITY excellence Awards

Retina - Démo



eEye® Digital Security

Merci

eEye® Digital Security

Pour plus d’information

Edouard Lorrain : elorrain@eeye.com
Benoît Roussel : broussel@eeye.com

01 58 71 40 31
www.eeye.com

eEye® Digital Security