i-Watch

Analyse et contrôle de vos applications Web

Bénéfices

- **Visibilité**
  Découverte et analyse des niveaux de sécurité
- **Sensibilisation**
  Explication des risques et des conséquences potentielles
- **Maîtrise des risques**
  Préconisation de remèdes
- **Flexibilité**
  Contrôle permanent et transparent

Mieux connaître ses applications

Le rôle stratégique occupé par les applications Web ne fait que croître. Souplesse, réactivité et performance, les avantages sont nombreux. Mais cette évolution n'est pas sans conséquence pour les services informatiques qui doivent gérer et sécuriser des applications dont ils n'ont souvent qu'une connaissance imparfaite : la différence de métiers, de culture et d'objectifs, ainsi que l'origine souvent externe des développements représentent autant d'obstacles.

Les deux premiers éléments de réponse s'appellent connaissance et compréhension. Quels sont les enjeux de la sécurité applicative, où sont les points sensibles et pourquoi ? Quels sont les traitements possibles ?

Voilà autant d'aspects que l'Entreprise va devoir appréhender, non de façon théorique et générique mais au contraire avec des réponses personnalisées, application par application. En d'autres termes construire pas à pas sa propre politique de sécurité applicative.

Suivre leur utilisation et leurs évolutions

Simple et rapide à mettre en oeuvre parce que basée sur l'observation du trafic, la solution i-Watch va reconnaître, analyser et classifier les différentes ressources mises en oeuvre par les applications. Ce rôle d'information est complété par un rôle pédagogique. Grâce à la base de connaissance intégrée i-Watch va alors renseigner l'Administrateur sur les risques induits pour ensuite l'orienter vers les différents remèdes possibles.

Parce que l'univers du Web est en permanente évolution, la solution i-Watch est conçue pour accompagner les applications tout au long de leur cycle de vie, de la préparation au déploiement jusqu'à la supervision des modifications. Son activité de monitoring va d'une part automatiquement détecter les changements apportés à la structure de l'application et d'autre part superviser son trafic et alerter les responsables en cas d'anomalies ou d'attaques.

contact@bee-ware.net • www.bee-ware.net
FRANCE : **+33 (0)1 41 03 14 83**

À propos de Bee Ware :

Bee Ware est un éditeur spécialisé dans la sécurisation et l'optimisation des applications Web. Disponibles sous forme d'Appliance, les solutions Bee Ware garantissent à la fois les performances et la confiance permettant de bénéficier des technologies Web en toute sérénité.

BeeWare
Delivering Confidence in Web Applications

i-Watch

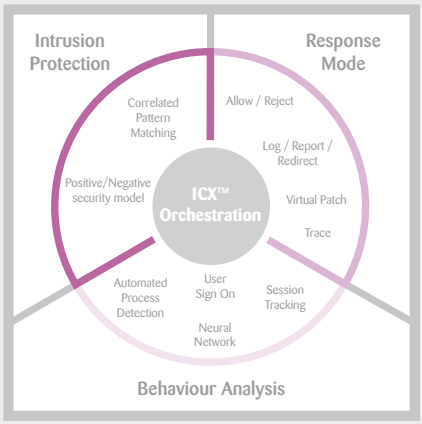
Technologie ICX™

- ICX est une intelligence d'analyse de Sécurité Web. Sa fonction est d'analyser l'utilisation d'une application sous l'angle de la sécurité, de classifier le trafic mis en œuvre, d'en détecter la dangerosité et d'appliquer ensuite le traitement approprié.
- ICX est constitué autour d'un centre d'orchestration qui va orienter et appliquer une analyse en fonction de critères contextuels.
- ICX orchestre un ensemble extensible d'algorithmes d'analyse :

-Détection d'intrusion
White List - Black List
Pattern Matching

-Analyse comportementale
Réseau de Neurones
Session Tracking
Cookie Poisoning
Dynamic White List (DWL)

Le mode de réponse le plus approprié est choisi à l'aide d'une représentation graphique matricielle familière à tous les administrateurs de règles de sécurité. ICX 2.0 supporte actuellement :
- Autorisation, Rejet, Redirection
- Ré-écriture de requête entrante ou sortante
- Emission de message d'erreur



Caractéristiques

Gamme de 3 modèles selon performance
Appliance format 1U ou 2U
Sniffer transparent (L2) intégré
Management Web (SSL)
Supervision SNMP et Syslog
Reporting PDF, HTML, XML

Fonctionnalités

Qualification

Cartographie de l'application
Identification des ressources :
- Détection des scripts sensibles
- Détection des applications sensibles
- Détection des ressources ambigües
- Détection des artefacts indésirables

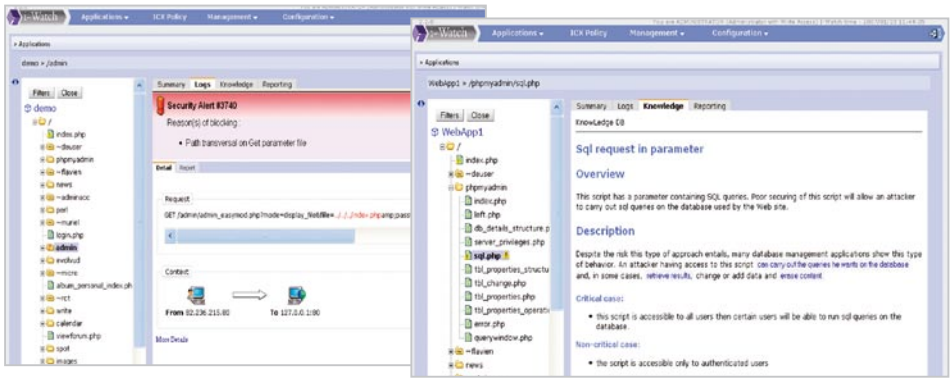
Identification des risques

Analyse des ressources sensibles
Mise en évidence des paramètres incriminés
Évaluation des risques potentiels

Monitoring

Support de différents modes de lecture du trafic :
- Lecture en temps réel basée sur un sniffer en mode transparent
- Lecture des fichiers logs de serveurs Web
- Lecture de fichier TCP/Dump
- Lecture des logs i-Sentry et i-Trust

Détection des attaques
Détection des comportements automatisés



Reporting

Les fonctions de reporting fournies avec i-Watch sont particulièrement riches et évoluées :

- Analyse de la dangerosité des requêtes
- Explication des vulnérabilités
- Préconisation de correctifs
- Rapport de risques
- Rapport d'attaques
- Rapport de ressources critiques

Les rapports générés par i-Watch ont été conçus pour répondre de façon spécifique aux questions posées par différentes populations de l'Entreprise : administrateurs, développeurs et décideurs.