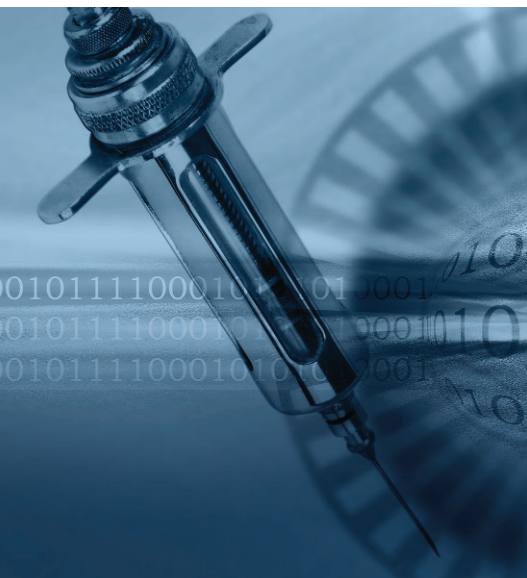


Digital Vaccine®

FICHE TECHNIQUE



Filtres Digital Vaccine

- Signatures
- Vulnérabilités
- Anomalies protocolaires
- Anomalies du trafic

Sécurité automatique

- « Paramètres conseillés » pour les filtres
- Plus de 600 filtres activés par défaut en mode blocage, à la livraison
- Mise à jour automatique hebdomadaire

Une réputation d'expert sécurité partout dans le monde

L'équipe Digital Vaccine de TippingPoint développe en permanence des filtres de protection pour résoudre les problèmes causés par les failles, virus, vers, chevaux de Troie, logiciels de P2P, spyware et autres, et les intégrer à Digital Vaccine. Chaque semaine, une nouvelle version de Digital Vaccine, contenant les tout derniers filtres, est communiquée automatiquement aux abonnés.

La précision et la pertinence des filtres Digital Vaccine de TippingPoint sont le fruit de la perspicacité et de l'expérience hors pair des spécialistes de Digital Vaccine.

TippingPoint a noué des relations étroites avec les fournisseurs et les entreprises afin de tout savoir sur les nouvelles failles découvertes avant qu'elles ne soient rendues publiques. De plus, l'équipe Digital Vaccine de TippingPoint étudie les listes de diffusion spécialisées dans les problèmes de sécurité, surveille les chat rooms des pirates, repère les attaques encore non identifiées et met à profit son immense réseau pour identifier à tout moment les risques les plus sérieux. Dans tous les cas, l'équipe vérifie et reproduit les failles nouvellement découvertes. Elle les examine avec soin, dans l'environnement contrôlé d'un laboratoire tout entier consacré à la sécurité, de manière à repérer d'autres vecteurs d'attaque potentiels.

Ainsi, les filtres Digital Vaccine sont conçus pour combattre à la fois des risques spécifiques mais aussi toutes leurs permutations potentielles. Ils sont envoyés à nos clients chaque semaine, ou dès l'apparition d'une faille critique, et peuvent être déployés automatiquement, sans intervention de l'utilisateur.

Les produits Tipping Point fournissent une protection couvrant tous les types de filtres qu'on peut regrouper en quatre catégories :

L'analyse des signatures vous protège contre les risques tels que virus et chevaux de Troie. Les filtres permettent d'identifier l'attaque et peuvent détecter l'agresseur sous sa forme exécutable.

L'analyse des vulnérabilités vous protège des failles des systèmes d'exploitation et applications. Les filtres ne dépendent pas d'une catégorie précise d'attaque. Ils jouent le rôle de correctif logiciel virtuel et défendent les hôtes contre les attaques ciblées sur des vulnérabilités non corrigées du réseau.



L'analyse des anomalies protocolaires permet de définir des filtres sous la forme de règles servant à détecter des conditions en contravention avec l'utilisation normale d'une application (p. ex., un dépassement de tampon) ou la spécification d'un protocole (p. ex., une anomalie RFC).

L'analyse des anomalies du trafic est utilisée pour détecter les modifications dans les schémas habituels de circulation du trafic. Les filtres dits adaptatifs apprennent le comportement « normal » du trafic dans l'environnement particulier où est installé l'IPS TippingPoint. Une fois le trafic « normal » modélisé, ils détectent les anomalies statistiques en fonction de seuils réglables. Ces filtres sont efficaces contre les attaques distribuées de type déni de service, les vers inconnus, les applications pirates et autres attaques de type ZDE. Facteur déterminant, l'IPS est capable de mettre en forme les débits des flux de trafic en fonction des types d'application, protocoles ou adresses IP.

Des tests réalisés par des cabinets indépendants ont montré que les produits TippingPoint offrent une meilleure couverture des failles que n'importe lequel de nos concurrents. Au cours des tests du NSS Group, TippingPoint a été le seul fournisseur à obtenir un score parfait de 100% pour la détection des attaques, les évasions et dans toutes les catégories de tests de sécurité réalisés.

Une couverture complète
TippingPoint propose la protection par IPS la plus complète du marché et la plus pertinente en terme de temps de réaction.

TippingPoint développe et publie des mises à jour de ses filtres qui couvrent toutes les failles et les risques pour la sécurité des réseaux identifiés dans le monde. Sans se limiter à un nombre restreint de problèmes, les packages Digital Vaccine de TippingPoint répondent à toutes les vulnérabilités et toutes les menaces identifiées. Les filtres Digital Vaccine assurent une protection totale du réseau contre tous les trafics préjudiciables.

TippingPoint est également le principal contributeur au bulletin électronique @RISK coordonné par le SANS Institute et qui regroupe les dernières informations sur les failles de sécurité des réseaux. Diffusé tous les jeudis auprès de quelques 300 000 abonnés dans le monde, pour la plupart spécialistes de la sécurité des réseaux, @RISK décrit les dernières failles découvertes, explique leur impact et les actions qu'ont initié les grandes entreprises pour protéger leurs utilisateurs. @RISK peut être obtenu gratuitement sur <http://www.sans.org/newsletters/risk/>.

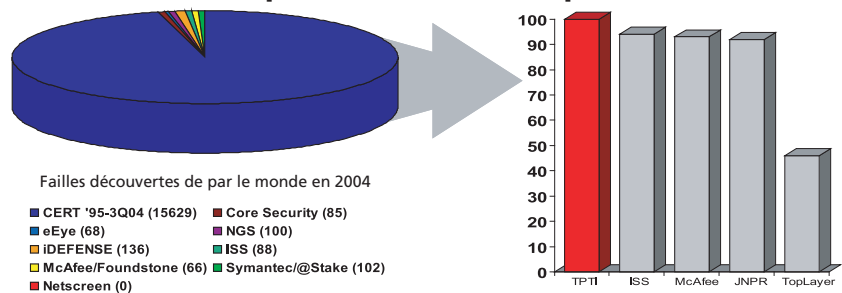
Une réponse rapide aux attaques ZDE
La réponse de TippingPoint aux attaques ZDE n'a pas d'équivalent sur le marché. Ici, la vitesse de réaction est cruciale, dans la mesure où l'apparition des attaques est de plus en plus rapide.

C'est en octobre 2004 que Microsoft a publié le plus grand nombre de bulletins de sécurité dans son histoire. TippingPoint a systématiquement communiqué à ses clients une mise à jour de Digital Vaccine apte à assurer leur protection face au nouveau problème dans les douze heures suivant la publication du bulletin. Il a chaque fois fallu plusieurs jours aux attaques pour se manifester.

Le 24 décembre 2004, deux nouvelles vulnérabilités ZDE ont été découvertes chez Microsoft (Internet Explorer HTML Help ActiveX Code Execution et Loadimage DLL Buffer Overflow). Même pendant les fêtes, il n'a fallu que quelques heures à TippingPoint pour proposer une mise à jour automatique des filtres de ses systèmes IPS. Ces mêmes filtres protégeaient déjà nos clients du cheval de Troie Phel, apparu le lendemain et qui exploitait largement l'une des nouvelles failles.

Les mises à jour de Digital Vaccine Le SMS TippingPoint (système d'administration de la sécurité) recherche en permanence de nouvelles mises à jours de Digital Vaccine au sein de notre Centre de gestion des risques. Lorsqu'une telle mise à jour est disponible, le système invite l'utilisateur à l'installer ou la télécharge et l'active automatiquement, selon l'option choisie.

TippingPoint : Une couverture de 100% vérifiée par des tests indépendants



TippingPoint assure une protection intégrale sur un vaste spectre de vulnérabilités. Les équipes de recherche de la plupart des sociétés ne s'intéressent qu'à un faible pourcentage des failles découvertes, d'où les insuffisances de leur couverture.