Sourcefire : 1er Next-Generation IPS avec contrÃ´le des applications
Logiciel
PostÃ© par : JerryG
PubliÃ©e le : 29/2/2012 15:00:00

GrÃ¢ce Ã une connaissance du contexte et Ã ses capacitÃ©s d'ajustement, **la solution NGIPS de Sourcefire** offre une visibilitÃ© accrue et une automatisation de la sÃ©curitÃ© adaptative.

Sourcefire Inc. , acteur majeur sur le marchÃ© des solutions de cybersÃ©curitÃ© adaptatives (Intelligent Cybersecurity solutions), annonce le premier Next-Generation Intrusion Prevention System (NGIPS) qui intÃ¨gre un contrÃ´le des applications adaptatif. Sourcefire, Ã©diteur pionnier sur le marchÃ© NGIPS depuis 2003, Ã©tend son concept Agile Securityâ¢ en proposant le premier NGIPS du marchÃ© qui offre une connaissance du contexte en temps rÃ©el, une visibilitÃ© des couches (Mac, IP, services, applications), ainsi qu'une automatisation de la sÃ©curitÃ© adaptative et un contrÃ´le des applications granulaire.

Le contrÃ´le des applications de Sourcefire permet aux entreprises de surveiller les accÃ¨s de milliers d'applications, y compris le contrÃ´le des applications propriÃ©taires. Il offre Ã©galement aux entreprises un contrÃ´le des menaces pour limiter le champ d'action des attaques et faire respecter les politiques de sÃ©curitÃ© mises en place. Avec la dÃ©tection et le contrÃ´le des applications dans une plateforme NGIPS universelle, les entreprises peuvent facilement Ã©tablir des politiques de sÃ©curitÃ© intÃ©grÃ©es pour Ã©quilibrer les mesures de contrÃ´le d'accÃ¨s avec une prÃ©vention des menaces efficace afin de traiter de maniÃ¨re globale les risques sur les couches applicatives.

Sourcefire NGIPS est construit sur la plateforme haute performance FirePOWERâ¢. En plus du contrÃ´le applicatif, la derniÃ¨re version NGIPS de Sourcefire inclut la technologie FireSIGHTâ¢ qui offre une connaissance du contexte, capable de s'adapter Ã l'environnement Ã©volutif de l'entreprise.

FireSIGHT fournit :

- Une connaissance et un contrÃ´le sur des milliers d'applications, y compris les applications clients, les applications web et les applications virtualisÃ©es

- Une visibilitÃ© en temps rÃ©el sur l'ensemble du SI : serveurs d'hÃ©bergement, applications, comportement des utilisateurs et infrastructure rÃ©seau

- Une cartographie du rÃ©seau et de l'infrastructure hÃ©bergÃ©e

- Une analyse du comportement du rÃ©seau et de la couche 7 avec une dÃ©tection des anomalies

- Une Ã©valuation automatique de l'impact des Ã©vÃ©nements de sÃ©curitÃ© pour filtrer les Â« bruits Â»

- Des recommandations automatiques des politiques de sÃ©curitÃ© basÃ©e sur la connaissance du contexte

Le reporting dÃ©diÃ© au contrÃ´le applicatif comprend des statistiques sur les applications pour une visibilitÃ© sur l'activitÃ© en termes de risques, d'hÃ©bergement, de consommation en bande passante, de version du navigateur... En outre, il est possible de crÃ©er facilement des rapports sur mesure et de mettre en place une rÃ©ception automatique des rapports par mail.

Â« *La lutte pour la sÃ©curitÃ© du rÃ©seau se joue sur le degrÃ© d'importance de l'information, dans laquelle deux des principes les plus critiques sont la visibilitÃ© et le contrÃ´le Â»,* explique **Martin Roesch**, Fondateur et CTO de Sourcefire. *Â« L'obstacle majeur pour dÃ©terminer le degrÃ© d'importance des donnÃ©es, c'est le rythme du changement de l'environnement, aussi bien que celui de l'informatique de l'entreprise que l'environnement plus global des menaces. Sourcefire offre la premiÃ¨re vÃ©ritable solution de dÃ©fense pour rÃ©pondre Ã ces deux dÃ©fis. Alors que d'autres fournisseurs sur le marchÃ© Ã©voluent dans un cadre prÃ©cis, notre solution bÃ©nÃ©ficie de multiples technologies qui fonctionnent en tandem afin de nous permettre tout d'abord de Â« voir Â» puis de Â« contrÃ´ler Â» la menace pour dÃ©fendre l'information Â».*