Internet : Sourcefire, des firewalls nouvelle gÃ©nÃ©ration pour PME.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 28/10/2010 14:30:00

Sourcefire, Inc, acteur majeur le marchÃ© de la sÃ©curitÃ© informatique (Intelligent Cybersecurity solutions) et crÃ©ateur de SnortÂ® annonce aujourdâ□□hui son **entrÃ©e imminente sur le marchÃ© du firewall de nouvelle gÃ©nÃ©ration** (NGFW)

Il prÃ©sente Ã cette occasion trois nouvelles offres Â« Defense Center Awareness Bundles Â» qui sâ□□inscrivent pleinement dans la nouvelle gÃ©nÃ©ration de solutions de prÃ©vention dâ□□intrusions (NGIPS) de Sourcefire.

Ces solutions fournissent aux entreprises une protection complÃ¨te contre les menaces, grÃ¢ce Ã une sÃ©curisation du pÃ©rimÃ¨tre de lâ□□entreprise, du data center et du cloud.

GrÃ¢ce Ã sa technologie IPS de nouvelle gÃ©nÃ©ration et Ã ses technologies existantes autour de la dÃ©tection temps rÃ©el des applications, des systÃ¨mes dâ□□exploitation, des utilisateurs et des Ã©quipements, Sourcefire compte Ã©tendre son positionnement pour sâ□□inscrire sur le marchÃ© des firewalls de nouvelle gÃ©nÃ©ration. Cette extension se concentrera sur lâ□□amÃ©lioration de lâ□□identification et du contrÃ´le des applications â□□ assurant une meilleure protection par le biais de la gestion de politiques de lâ□□entreprise sur lâ□□usage des applications dans le rÃ©seau.

Â« *Je suis heureux dâ□□annoncer notre projet de dÃ©velopper notre marchÃ© vers le marchÃ© des firewalls de nouvelle gÃ©nÃ©ration en nous appuyant sur notre positionnement dâ□□IPS de nouvelle gÃ©nÃ©ration et sur nos technologies temps rÃ©el* Â» dÃ©clare **John Burris**, CEO de Sourcefire. Â« *En tant que pionnier dans la fourniture de solutions IPS intelligentes, Sourcefire bÃ©nÃ©ficie dâ□□un positionnement unique qui lui permet dâ□□ajouter de maniÃ¨re transparente des fonctionnalitÃ©s NGFW dans lâ□□ensemble de ses solutions* Â».

Disponibles immÃ©diatement, les offres Â« NGIPS Awareness Bundles de Sourcefire Â» facilitent lâ□□achat et lâ□□intÃ©gration des solutions tout en fournissant, comme les prÃ©cÃ©dentes solutions, une connaissance du rÃ©seau en temps rÃ©el afin dâ□□identifier les menaces complexes persistantes (APT), une architecture ouverte pour permettre une

personnalisation en fonction de lâ□□environnement du client et lâ□□automatisation intuitive pour une Ã©valuation de lâ□□impact des attaques et tuning automatique de lâ□□IPS.

Â« *Sourcefire a comblÃ© un manque sur le marchÃ© de lâ□□IPS, lÃ ou les technologies classiques gÃ©nÃ¨rent souvent un nombre excessif dâ□□Ã©vÃ©nements de sÃ©curitÃ© et proposent une architecture fermÃ©e qui oblige les utilisateurs Ã accepter les rÃ¨gles par dÃ©faut,*Â» affirme **Charles Kolodgy**, Vice PrÃ©sident de la recherche chez IDC. Â« *Les dÃ©fenses statiques sont incapables de protÃ©ger le rÃ©seau contre les menaces dynamiques dâ□□aujourdâ□□hui. Lâ□□IPS de nouvelle gÃ©nÃ©ration de Sourcefire est intelligent, adaptatif et automatisÃ©, donnant aux utilisateurs une visibilitÃ© en temps rÃ©el sur ce qui est prÃ©sent sur leurs rÃ©seaux, ce qui est vulnÃ©rable et ce qui pourrait Ãªtre attaquÃ©.*â□□

Les avantages qui diffÃ©rencient lâ□□IPS de nouvelle gÃ©nÃ©ration de Sourcefire :

i□· Une connaissance du contexte â□□ La combinaison entre la visibilitÃ© temps rÃ©el du rÃ©seau, des applications, des comportements et des identitÃ©s des utilisateurs pour une sÃ©curitÃ© optimale face aux menaces Ã©volutives.

i□· Une architecture ouverte â□□ Permet aux utilisateurs de crÃ©er facilement des rÃ¨gles personnalisÃ©es pour leur environnement. Les utilisateurs de lâ□□IPS de nouvelle gÃ©nÃ©ration de Sourcefire peuvent Ã©galement compter sur la collaboration et lâ□□innovation de la communautÃ© Snort pour la mise Ã jour des rÃ¨gles et de lâ□□Ã©quipe VRT de Sourcefire pour la recherche des vulnÃ©rabilitÃ©s.

i□· Une automatisation intelligente â□□ La technologie Sourcefire sâ□□appuie sur la connaissance du contexte en temps rÃ©el afin dâ□□automatiser Ã la fois lâ□□Ã©valuation de lâ□□impact et la mise au point de lâ□□IPS. Les NGIPS de Sourcefire utilisent la connaissance de la cartographie rÃ©seau en temps rÃ©el pour corrÃ©ler automatiquement les attaques aux vulnÃ©rabilitÃ©s potentielles, pour gÃ©rer les politiques et pour rÃ©duire de maniÃ¨re importante le nombre dâ□□Ã©vÃ©nements de sÃ©curitÃ© Ã traiter.