Blue Coat : une nouvelle solution de protection contre les menaces complexes en PME
Logiciel
PostÃ© par : JPilo
PubliÃ©e le : 19/11/2013 13:30:00

Blue Coat Systems Inc., leader sur le marchÃ© de la Business Assurance Technology, dÃ©voile sa **nouvelle solution Blue Coat Advanced Threat Protection** spÃ©cialement conÃ§ue afin de solidariser les opÃ©rations quotidiennes des professionnels de la sÃ©curitÃ©, la maÃ®trise et la rÃ©solution des incidents.
Cette nouvelle solution est la premiÃ¨re Ã proposer un systÃ¨me complet de dÃ©fense livrant une protection contre les menaces complexes adaptÃ©e Ã l'ensemble de leur cycle de vie, et permettant de fortifier le rÃ©seau en identifiant les attaques ciblÃ©es et complexes et les programmes malveillants de type zero-day. Dans le mÃªme temps, Blue Coat Advanced Threat Protection assure Ã©galement la mise en Å□uvre automatisÃ©e de meilleures pratiques de maÃ®trise des incidents avancÃ©s dans les cas oÃ¹ les menaces ne sont pas dÃ©tectÃ©es par les outils de sÃ©curitÃ© traditionnels. Les Ã©quipes chargÃ©es des opÃ©rations quotidiennes de gestion de la sÃ©curitÃ© et celles chargÃ©es des opÃ©rations plus complexes de sÃ©curitÃ© peuvent ainsi travailler ensemble Ã la protection et afin de laisser plus d'autonomie Ã l'ensemble de l'entreprise.

Les entreprises contemporaines font face Ã des failles de sÃ©curitÃ© matÃ©rielles en raison de la frontiÃ¨re structurelle entre les Ã©quipes chargÃ©es des opÃ©rations de sÃ©curitÃ© quotidiennes et celles chargÃ©es des opÃ©rations complexes de gestion de la sÃ©curitÃ©. Selon le rapport Verizon Data Breach sur la fuite de donnÃ©es, il suffit de quelques secondes, minutes ou heures Ã 84 % des attaques ciblÃ©es et complexes pour compromettre la sÃ©curitÃ© de leurs cibles, tandis que 78 % des violations prennent des semaines, des mois voire des annÃ©es Ã Ãªtre dÃ©couvertes. Cette diffÃ©rence provient du fait que les systÃ¨mes de dÃ©fense classiques sont conÃ§us pour dÃ©tecter et bloquer des menaces connues, mais sont globalement incapables de dÃ©tecter les menaces zero-day et les nouveaux programmes malveillants. Ce problÃ¨me est aggravÃ© par la tendance des Ã©quipes responsables des opÃ©rations complexes de sÃ©curitÃ© (et de leurs systÃ¨mes de dÃ©fense) Ã opÃ©rer de faÃ§on cloisonnÃ©e, sans possibilitÃ© de partage d'information avec les diffÃ©rentes entitÃ©s en charge de la sÃ©curitÃ©.

La nouvelle solution Blue Coat Advanced Threat Protection automatise et aligne les meilleures pratiques et les technologies avec les processus mÃ©tier et la politique de l'entreprise, de sorte que l'ensemble du service en charge de la sÃ©curitÃ© puisse dÃ©tecter, maÃ®triser et rÃ©soudre les menaces complexes rapidement, dÃ¨s que nÃ©cessaire et efficacement. Cette solution combine parfaitement les informations dÃ©cisionnelles en local et du monde entier sur les menaces afin d'identifier les programmes inconnus, et ce, Ã chaque Ã©tape du cycle de vie d'un incident (amÃ©liorant ainsi l'efficacitÃ© globale de l'infrastructure de sÃ©curitÃ©).

Â« *L'adoption en entreprise de nouvelles technologies s'Ã©tant accÃ©lÃ©rÃ©e pour l'ensemble des mÃ©tiers, il est de plus en plus important que les Ã©quipes chargÃ©es de la sÃ©curitÃ© comprennent qu'un certain nombre de menaces passeront Ã travers leurs systÃ¨mes de dÃ©fense prÃ©ventifs, et s'alignent afin de gÃ©rer ces menaces complexes Ã l'aide d'un systÃ¨me de dÃ©fense permettant de prendre des mesures sur l'intÃ©gralitÃ© de leur cycle de vie* Â», explique **Greg Clark**, CEO de **Blue Coat Systems**. Â« *La solution Blue Coat Advanced Threat Protection permet d'aligner les diffÃ©rentes Ã©quipes chargÃ©es de la sÃ©curitÃ© sur la stratÃ©gie, le processus et les mesures adÃ©quates avant, pendant et Ã la suite d'un problÃ¨me de sÃ©curitÃ©. Nos clients peuvent ainsi continuer Ã adopter de nouvelles technologies tout en garantissant la sÃ©curitÃ© de leur entreprise.* Â»

La solution Blue Coat Advanced Threat Protection automatise et dÃ©ploie une technologie Blue Coat Ã chaque Ã©tape du cycle de vie d'un incident. Elle s'appuie sur des meilleures pratiques

validÃ©es par l'industrie dans le cycle de gestion dÃ©fini par le National Institue of Standard and Technology (NIST) pour la maÃ®trise, l'Ã©radication et la reprise aprÃ¨s incident.

La solution livre des technologies de :

1) DÃ©tection et protection : pour la prÃ©vention contre les menaces dans le cadre des opÃ©rations quotidiennes, la passerelle Blue Coat Secure Web Gateway protÃ¨ge en temps rÃ©el contre les menaces connues, les sources malveillantes et les rÃ©seaux de diffusion de programmes malveillants. Le nouveau Blue Coat Content Analysis System permet d'orchestrer la protection contre les programmes malveillants et la mise d'applications sur liste blanche au niveau de la passerelle Internet, permettant ainsi aux Ã©quipes chargÃ©es de la sÃ©curitÃ© de gÃ©rer simplement les types d'activitÃ© Web autorisÃ©s ou non par les systÃ¨mes de sÃ©curitÃ© prÃ©ventifs. Des informations contextuelles sur les nouvelles menaces sont enregistrÃ©es localement et partagÃ©es/rÃ©cupÃ©rÃ©es en permanence dans le monde entier au sein d'une boucle de rÃ©troaction afin d'Ã©tendre les connaissances sur le menaces et le champ de protection fourni par le rÃ©seau Blue Coat Global Intelligence Network, qui compte 15 000 clients et plus de 75 millions d'utilisateurs.

2) Analyse et maÃ®trise : la solution Blue Coat Content Analysis System remonte les Ã©vÃ©nements inconnus afin de maÃ®triser les incidents survenus grÃ¢ce Ã ses fonctionnalitÃ©s d'analyse et de mise en bac Ã sable des programmes malveillants, ainsi que grÃ¢ce Ã la plateforme Security Analytics et Ã ses ThreatBLADES intÃ©grÃ©es. Le comportement et les caractÃ©ristiques d'une menace inconnue Ã©tant dÃ©couverts grÃ¢ce Ã une analyse automatisÃ©e, les informations rÃ©coltÃ©es sont ensuite partagÃ©es avec l'ensemble de l'infrastructure de sÃ©curitÃ©, ce qui permet d'amÃ©liorer la protection au niveau de la passerelle et de bÃ©nÃ©ficier d'une dÃ©fense plus adaptÃ©e et Ã©volutive. La technologie d'analyse de logiciels malveillants de Blue Coat s'intÃ¨gre Ã©galement aux environnements de sÃ©curitÃ© existants et peut faire office de courtier de solutions de bac Ã sable tierces, permettant ainsi aux clients d'en choisir une ou plusieurs pour la dÃ©tection des programmes malveillants complexes ou inconnus.

3) Examen et rÃ©solution : la plateforme Blue Coat Security Analytics Platform by Solera permet le profilage des menaces complexes et la rÃ©solution des incidents. Les informations sur les menaces connues sont utilisÃ©es pour examiner et contrer l'attaque dans son intÃ©gralitÃ©, y compris en tenant compte des autres instances de fichiers malveillants et des menaces dÃ©jÃ prÃ©sentes sur le rÃ©seau. Ces informations sont ensuite partagÃ©es avec l'ensemble de l'infrastructure de l'entreprise, ainsi que sur le rÃ©seau Blue Coat Intelligence Network afin d'automatiser la dÃ©tection des nouvelles menaces identifiÃ©es lors de la phase de Â« dÃ©tection et protection Â».

Â« *Les approches isolÃ©es de dÃ©tection des menaces complexes ou spÃ©cialisÃ©es sont difficiles Ã appliquer en raison des informations en corrÃ©lation dispersÃ©es au sein de l'infrastructure de sÃ©curitÃ©* Â», explique **Phil Hochmuth,** responsable du programme de recherche sur la sÃ©curitÃ© chez IDC. Â« *Afin de dÃ©tecter et de bloquer de telles attaques, les entreprises doivent adopter une approche de sÃ©curitÃ© intÃ©grÃ©e en reliant les diffÃ©rents centres d'informations sur les menaces au sein de leur infrastructure, afin d'accÃ©lÃ©rer la dÃ©tection des anomalies et la rÃ©solution des incidents en matiÃ¨re de sÃ©curitÃ©.* Â»