CyberArk Privileged Threat Analytics : pour dÃ©tecter les attaques en cours.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 20/11/2013 11:30:00

CyberArk, lâexpert de la sÃ©curitÃ© au cÅur des entreprises, a annoncÃ© le **lancement de Privileged Threat Analytics**â¢, la toute premiÃ¨re solution de traitement analytique capable de dÃ©tecter les comportements malveillants sur les comptes Ã privilÃ¨ges et dâinterrompre les attaques en cours, avant quâelles nâimpactent les activitÃ©s dâune organisation.

Les comptes Ã privilÃ¨ges sont connus pour Ãªtre une cible de choix des attaques avancÃ©es, menÃ©es de lâextÃ©rieur ou au sein mÃªme des organisations. Selon le cabinet de conseil en sÃ©curitÃ© Mandiant, Â« *les intrusions liÃ©es aux menaces persistantes avancÃ©es (APT : Advanced Persistent Threats) ciblent de prÃ©fÃ©rence les comptes Ã privilÃ¨ges tels que ceux des administrateurs de domaines, les comptes de services Ã privilÃ¨ges, les comptes dâadministrateurs locaux, ainsi que des utilisateurs des comptes Ã privilÃ¨ges* Â».

Privileged Threat Analytics de CyberArk fournit une analyse ciblÃ©e et concrÃ¨te des menaces et des vecteurs critiques dâattaques, permettant ainsi aux Ã©quipes de sÃ©curitÃ© de rÃ©agir et de neutraliser instantanÃ©ment une intrusion en cours.

Â La nouvelle offre de CyberArk est la seule solution dâanalyse des menaces ciblÃ©es des comptes Ã privilÃ¨ges.
Â« *Les comptes Ã privilÃ¨ges sont les comptes les plus puissants au sein des entreprises en raison de lâaccÃ¨s Ã©tendu quâils offrent. Pour nous, gÃ©rer et contrÃ´ler cet accÃ¨s est essentiel pour la sÃ©curisation de lâentreprise ainsi que pour la mise en place et le respect des rÃ¨gles de conformitÃ© de nombreuses rÃ©gulations*, explique **Erica Beall**, Analyste des systÃ¨mes de sÃ©curitÃ© informatique chez The Williams Companies. *Lâanalyse et les alertes en temps rÃ©el sur les activitÃ©s des utilisateurs de comptes Ã privilÃ¨ges permettront une meilleure gestion de nos systÃ¨mes grÃ¢ce Ã des informations impactantes qui renforceront au maximum notre positionnement sur la sÃ©curitÃ©.* Â»

Les avantages de CyberArk Privileged Threat Analytics: â¢ Identification des attaques externes en cours et du comportement suspect/malveillant dâune personne interne Ã lâentreprise.
â¢ DÃ©tection en temps rÃ©el dâun large Ã©ventail dâanomalies basÃ©es sur le comportement des personnes disposant de comptes Ã privilÃ¨ges, Ã lâimage dâun utilisateur qui tente dâaccÃ©der Ã un compte avec ses identifiants Ã un horaire inhabituel de la journÃ©e. Ceci peut indiquer une possible activitÃ© malveillante ou la transgression dâune rÃ¨gle de sÃ©curitÃ©, comme celle qui prohibe le partage des mots de passe.
â¢ Meilleure efficacitÃ© des systÃ¨mes SIEM et des Ã©quipes de sÃ©curitÃ© opÃ©rationnelle, grÃ¢ce Ã un faible nombre de faux-positifs.
â¢ Neutralisation rapide des attaques en cours pour maÃ®triser les dÃ©lais et les coÃ»ts de

rÃ©paration.
â¢ Identification et analyse permanente des comportements des utilisateurs privilÃ©giÃ©s autorisÃ©s et ajustement de lâÃ©valuation des risques sur la base de ces comportements.

Â« *DÃ©terminer le type de comportements des utilisateurs de comptes Ã privilÃ¨ges reprÃ©sente une arme de poids dans le combat des menaces internes et externes grÃ¢ce Ã la dÃ©tection rapide de comportements anormaux*, confie **Charles Kolodgy**, Vice-PrÃ©sident de la Recherche au service des Produits de SÃ©curitÃ© chez IDC. *Le secret de la nouvelle solution de CyberArk repose sur lâanalyse des bonnes donnÃ©es â notamment les activitÃ©s des utilisateurs de comptes Ã privilÃ¨ges â ce qui apporte une rÃ©elle valeur ajoutÃ©e, et des informations concrÃ¨tes sur les vecteurs dâattaques critiques.* Â»

Le nouveau champ de bataille de la sÃ©curitÃ© : le rÃ©seau interne
Le pÃ©rimÃ¨tre traditionnel de sÃ©curitÃ© nâest plus dâactualitÃ© et câest dÃ©sormais au sein du rÃ©seau que se joue la bataille pour la sÃ©curitÃ©. Privileged Threat Analytics est la toute derniÃ¨re innovation de CyberArk pour sÃ©curiser les comptes Ã privilÃ¨ges, et ainsi protÃ©ger les ressources et donnÃ©es des entreprises. Privileged Threat Analytics applique une technologie analytique brevetÃ©e qui analyse lâutilisation des comptes Ã privilÃ¨ges en corrÃ©lation avec des informations contextuelles issues des ressources systÃ¨mes. Il en rÃ©sulte une veille ciblÃ©e et pertinente qui facilite la prise de dÃ©cision au sein des Ã©quipes de sÃ©curitÃ©.

Â« *Les organisations doivent partir du principe que les assaillants sont dÃ©jÃ Ã lâintÃ©rieur de leur systÃ¨me et quâils tenteront en premier lieu de prendre le contrÃ´le des comptes Ã privilÃ¨ges*, explique **Roy Adar**, Vice-prÃ©sident en charge du Product Management chez **CyberArk**. *Nos clients souhaitent contrÃ´ler les comptes Ã privilÃ¨ges afin de pouvoir dÃ©tecter les activitÃ©s suspectes et protÃ©ger leur organisation contre des menaces en Ã©volution constante* Â».

CyberArk Privileged Threat Analytics sera disponible dÃ¨s dÃ©cembre 2013.