La visibilitÃ© au service de la protection en ligne
Internet
PostÃ© par : JerryG
PubliÃ©e le : 4/8/2023 13:00:00

Selon le dernier rapport Â« Worldwide Security Spending Guide Â» publiÃ© par IDC plus tÃ´t cette annÃ©e, les dÃ©penses mondiales en solutions et services de sÃ©curitÃ© devraient s'Ã©lever Ã 219 milliards de dollars en 2023, et les investissements dans les outils, les logiciels et les services de cybersÃ©curitÃ© devraient atteindre prÃ¨s de 300 milliards de dollars en 2026, en raison des cybermenaces constantes, des exigences liÃ©es aux environnements de travail hybrides et aux rÃ¨glementations en matiÃ¨re de confidentialitÃ© des donnÃ©es et de gouvernance.

En ligne, la protection parfaite nâ□□existe pas. Les cybercriminels sont en effet de plus en plus chevronnÃ©s et adoptent des techniques toujours plus sophistiquÃ©es, pour des surfaces dâ□□attaque qui augmentent de faÃ§on exponentielle. Face Ã ce paysage de menaces grandissant, les professionnels de la sÃ©curitÃ© doivent donc passer dâ□□une idÃ©ologie purement prÃ©ventive Ã une approche axÃ©e sur la dÃ©tection prÃ©coce et la rÃ©activitÃ©.

Ainsi, pour Philippe Alcoy, spÃ©cialiste sÃ©curitÃ© chez NETSCOUT, il ne sâ□□agit pas pour les experts de la cybersÃ©curitÃ© dâ□□Ã©liminer tous les outils de prÃ©vention de leur arsenal, mais plutÃ´t dâ□□accepter le caractÃ¨re provisoire des victoires.

Â« Câ□□est une course sans fin dont les hackers remporteront inÃ©vitablement certaines Ã©tapes en accÃ©dant aux rÃ©seaux des entreprises. La seule faÃ§on pour les organisations dâ□□amÃ©liorer leur posture de sÃ©curitÃ© consiste donc Ã se doter de la capacitÃ© de dÃ©tecter, au plus tÃ´t, tout comportement suspect afin dâ□□en dÃ©terminer la nature et de le neutraliser, le cas Ã©chÃ©ant, dans les meilleurs dÃ©lais.

Les failles sont vouÃ©es Ã survenir quoi quâ□□il arrive dans le cycle de vie dâ□□un rÃ©seau, mais câ□□est la rÃ©activitÃ© qui fait la diffÃ©rence. En effet, chaque fois quâ□□une violation majeure est dÃ©couverte, nos analyses montrent que les attaquants, la plupart du temps, se sont infiltrÃ©s insidieusement dans les rÃ©seaux et ont eu accÃ¨s aux systÃ¨mes ciblÃ©s pendant des semaines, voire des mois, avant dâ□□Ãªtre dÃ©tectÃ©s.

Aux sempiternelles questions relatives Ã la remÃ©diation ou aux outils et mÃ©thodes qui aideront les Ã©quipes IT Ã dÃ©tecter plus rapidement les comportements suspects, une seule rÃ©ponse prÃ©vaut : la visibilitÃ©. Elle est impÃ©rative car on ne peut pas sÃ©curiser ce que lâ□□on ne peut pas voir.

Gartner a prÃ©sentÃ© sa Â« triade de la visibilitÃ© Â» dans un rapport intitulÃ© Applying Network-Centric Approaches for Threat Detection and Response (Application dâ□□approches axÃ©es sur le rÃ©seau pour la dÃ©tection et la rÃ©ponse aux attaques).

Lâ□□analyste estime ainsi que : Â« La sophistication croissante des attaques oblige les entreprises Ã utiliser de multiples sources de donnÃ©es pour les dÃ©tecter et y rÃ©agir. Les technologies basÃ©es sur les rÃ©seaux permettent aux techniciens spÃ©cialisÃ©s dâ□□obtenir rapidement une visibilitÃ© sur les menaces dans lâ□□ensemble dâ□□un environnement sans faire appel Ã des agents. Â» Ces outils : le SIEM, lâ□□EDR et la NDR, prÃ©sentent de nombreux avantages et se sont ainsi rÃ©vÃ©lÃ©s complÃ©mentaires.

â□¢ Le SIEM (systÃ¨me de gestion des Ã©vÃ©nements et des informations de sÃ©curitÃ©)

recueille et analyse des donnÃ©es de logs, câ□□est-Ã -dire des listes dâ□□Ã©vÃ©nements sâ□□Ã©tant produits dans un systÃ¨me informatique, tels que des connexions, des erreurs ou tout autre problÃ¨me.

Si ces donnÃ©es sont collectÃ©es sur de longues pÃ©riodes (Ã partir dâ□□un ou deux ans, par exemple), il est alors possible de crÃ©er ses propres rÃ¨gles de dÃ©tection personnalisÃ©es. Toutefois, ce systÃ¨me est extrÃªmement coÃ»teux et long Ã mettre en Å□uvre.

De plus, il nÃ©cessite un niveau dâ□□expertise Ã©levÃ© pour assurer la rÃ©daction des rÃ¨gles personnalisÃ©es. Mais la collecte de donnÃ©es de logs est importante pour permettre aux Ã©quipes informatiques de comprendre le fonctionnement de leurs systÃ¨mes, de les dÃ©panner ou mÃªme de les soumettre Ã un audit.

â□¢ Lâ□□EDR (dÃ©tection et rÃ©ponse au niveau des points dâ□□accÃ¨s) permet pour sa part de capturer lâ□□exÃ©cution, les connexions locales, les modifications dâ□□un systÃ¨me, ainsi que les activitÃ©s de la mÃ©moire et dâ□□autres opÃ©rations Ã partir des points dâ□□accÃ¨s.

Ces derniers dÃ©signent diffÃ©rents types de terminaux, tels que les serveurs, les ordinateurs portables ou encore les tÃ©lÃ©phones, lesquels sont les plus frÃ©quemment compromis par des utilisateurs distraits qui cliquent accidentellement sur un lien frauduleux, ne verrouillent pas leurs appareils ou ont recours Ã des codes confidentiels faibles, ou installent des applications ayant des vulnÃ©rabilitÃ©s non corrigÃ©es, telles que des logiciels obsolÃ¨tes.

Ces terminaux infectÃ©s se connectent sans difficultÃ© au rÃ©seau de lâ□□entreprise et donnent aux hackers malveillants la possibilitÃ© de sâ□□y dÃ©placer librement pour accÃ©der aux informations quâ□□ils convoitent.

â□¢ Enfin, la NDR (dÃ©tection et rÃ©ponse au niveau du rÃ©seau) assure la visibilitÃ© du rÃ©seau par le biais dâ□□outils conÃ§us pour la capture et lâ□□analyse du trafic. Les solutions NDR sâ□□avÃ¨rent Ãªtre lâ□□une des technologies les plus importantes de la pile de sÃ©curitÃ©, puisque les pirates doivent se connecter au rÃ©seau pour accÃ©der aux donnÃ©es visÃ©es.

Cependant le rÃ©seau reste le seul endroit oÃ¹ un attaquant ne peut cacher son activitÃ© dÃ¨s lors que lâ□□on peut saisir une capture de paquets (PCAP), qui contient une preuve objective en cas de violation potentielle. Certaines entreprises pensent quâ□□il suffit dâ□□avoir des solutions SIEM et EDR, mais ces angles morts rÃ©seau subsistent laissant des lacunes en matiÃ¨re de visibilitÃ©. La seule faÃ§on de bÃ©nÃ©ficier dâ□□une sÃ©curitÃ© complÃ¨te consiste Ã se doter dâ□□une solution de surveillance du rÃ©seau.

Chacune de ces solutions est nÃ©cessaire mais prÃ©sente ses propres inconvÃ©nients. Ainsi, les donnÃ©es de logs ne fournissent pas dâ□□informations vÃ©ritablement contextualisÃ©es, tandis que lâ□□EDR nÃ©cessite des centaines, voire des milliers dâ□□agents qui ne suivent pas toujours la sophistication croissante des logiciels malveillants, et dont lâ□□empreinte matÃ©rielle est souvent incompatible pour un dÃ©ploiement sur les appareils IoT.

Certaines solutions NDR prÃ©sentent elles aussi des inconvÃ©nients quant Ã la qualitÃ© des donnÃ©es. Câ□□est pourquoi, ces trois solutions de sÃ©curitÃ© peuvent et devraient Ãªtre complÃ©tÃ©es par un outil de visibilitÃ© de bout en bout qui permette la capture et lâ□□inspection approfondie des paquets (DPI) Ã grande Ã©chelle.

Cette approche permettra ainsi de disposer dâ□□une riche source de mÃ©tadonnÃ©es et offrira aux Ã©quipes IT la visibilitÃ© Ã la fois au point dâ□□intrusion et Ã lâ□□emplacement de la dÃ©tection.

Elles pourront ainsi examiner lâ□□incident avant, pendant et aprÃ¨s lâ□□attaque et disposeront des

moyens de neutraliser et de prÃ©venir toute menace future. De cette maniÃ¨re, elles seront plus Ã mÃªme de de garder une visibilitÃ© totale sur les rÃ©seaux, de dÃ©tecter toute activitÃ© inhabituelle et de garder une longueur dâ□□avance sur les cybercriminels. Â»Â