Automatisation de la réponse aux incidents avec Riverbed AppResponse

Les avertissements de sécurité, tels que ceux provenant d'un système de détection des intrusions ou d'un système d'alerte basé sur les journaux, n'annoncent pas toujours immédiatement la gravité d'un incident. Dans la plupart des cas, ces avertissements sont stockés et disponibles pour toute enquête ultérieure au cas où des informations supplémentaires seraient nécessaires. Malheureusement, de nombreux incidents de sécurité mettent des semaines, voire des mois, à se manifester, le « temps de séjour » des pirates ayant augmenté au cours des dernières décennies. Les API Riverbed AppResponse permettent de créer automatiquement des fichiers PCAP (capture de paquets) pertinents correspondant à tout événement d'intérêt. Cela signifie qu'un responsable de la sécurité disposera de tous les paquets pertinents pour tout événement lorsque le moment sera venu d'aller plus loin, et ce même si l'événement a eu lieu plusieurs mois auparavant.

Contexte

Cet acteur mondial et innovant dans le domaine de la biopharmacie déploie l'intégralité de la solution de gestion des performances réseau (NPM) unifiée de Riverbed, comprenant la surveillance des flux haute fidélité, la capture des paquets et la surveillance des terminaux, car il a compris l'adage : *ce qui ne peut pas être mesuré ne peut être géré*. Il croit également en son corollaire : *ce qui n'est pas visible ne peut être sécurisé*. Et c'est ce point que nous souhaitons développer aujourd'hui.

La capture et l'analyse des paquets de Riverbed AppResponse fournissent une télémétrie précieuse aux équipes responsables des opérations réseau et de sécurité. L'équipe responsable des opérations réseau peut exploiter les mesures TCP et le tableau de composition du temps de réponse pour enquêter sur les rapports relatifs aux problèmes de performances applicatives lentes, tandis que l'équipe en charge des opérations de sécurité peut exploiter les données de paquets stockées par AppResponse pour alimenter toute enquête de sécurité.

Les données de paquets sont essentiels pour la réponse aux incidents

En déployant AppResponse, l'objectif de ce client dans le domaine de la biopharmacie est de conserver 24 heures de données de paquets sur toute appliance AppResponse. L'équipe de sécurité peut avoir besoin d'un historique beaucoup plus long, particulièrement lorsque les paquets sont associés à des détections IDS/IPS/NDR, mais les paquets intéressants peuvent parfois avoir déjà dépassé le tampon de capture AppResponse.

La durée pendant laquelle une solution de capture de paquets peut stocker ces derniers dépend du volume de données capturées et du stockage disponible pour ces paquets sur l'appliance. Bien qu'AppResponse fournisse un contrôle granulaire des paquets qui doivent être stockés, il est possible que certains, bien que nécessaires pour résoudre un problème de performance ou une enquête de sécurité, ne soient pas disponibles. Augmenter la capacité de stockage de paquets permet d'allonger leur temps de conservation, certes, mais il existera toujours une limite au volume de données de paquets qui peuvent être conservées. Les services professionnels de Riverbed ont pu fournir une solution créative et efficace pour aider le client à exploiter au mieux le stockage de paquets disponible.

L'API automatise le stockage de paquets

Les services professionnels de Riverbed ont fourni à l'équipe de sécurité du client un processus de capture de paquets en deux étapes pour répondre aux incidents :

1. La création d'une API qui leur permet de demander des captures de paquets pour des adresses IP, des ports et des plages de temps spécifiques, de manière automatisée, en fonction des événements détectés par leurs outils de sécurité. Une requête faite à l'API retourne une liste d'appliances AppResponse contenant les paquets associés à cette même requête.
2. Une deuxième API formule une requête ultérieure à l'une des appliances AppResponse identifiées afin de récupérer les paquets d'intérêt. Elle enregistre ensuite les paquets sur un serveur FTP sécurisé pour analyse ultérieure.

Grâce au cadre de l'API en place, le client a également été en mesure de construire un réseau frontend pour l'équipe de sécurité et d'autres parties prenantes afin de demander des captures de paquets d'adresses IP et de ports spécifiques pour une période donnée. Une fois la requête programmée et traitée, l'utilisateur reçoit un e-mail l'informant que sa requête est finalisée et contenant un lien sécurisé vers l'emplacement de stockage des paquets demandés.

Bénéfices pour les parties prenantes

Cette solution innovante améliore l'agilité de l'équipe de sécurité et les capacités d'analyse scientifique en fournissant un processus automatisé pour préserver les preuves basées sur les paquets associées aux événements de sécurité et le support nécessaire pour une enquête de sécurité plus approfondie. Pour l'équipe en charge des outils, cette solution optimise le ROI d'AppResponse. Elle lui permet de répondre aux besoins de nouvelles parties prenantes en allongeant le temps de conservation des paquets sans avoir à investir dans des unités de stockage supplémentaires.