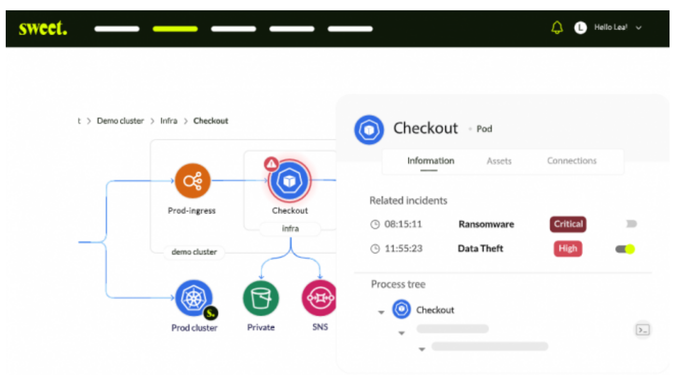
Sweet, un outil pour scanner les attaques de workloads cloud

Shweta Sharma, IDG NS (adapté par Célia Seramour) , publié le 25 Aout 2023

Les équipes de sécurité doivent s'armer d'outils en tout genre pour surveiller les attaques. Sweet, un logiciel de sécurité qui utilise la technologie eBPF pour analyser les anomalies d'exécution dans les environnements cloud pourrait être une arme de taille dans cette bataille.



Un aperçu de la plateforme Sweet développée par l'éditeur en cybersécurité Sweet Security. (Crédit : Sweet Security)

Le fournisseur de cybersécurité cloud Sweet Security a lancé une plateforme de sécurité d'exécution, baptisée Sweet, pour aider les équipes SSI à détecter les attaques basées sur le cloud et y répondre en temps réel. La plateforme déploie des capteurs dans l'environnement d'exécution pour fournir aux RSSI et aux équipes de sécurité une visibilité sur les clusters cloud.

« Comme les solutions de détection et de réponse traditionnelles, nous avons des capteurs déployés dans l'environnement cible », indique Eyal Fisher, chef de produit chez Sweet Security. « Mais notre capteur est conçu spécifiquement pour les charges de travail dans le cloud et les applications natives fonctionnant sur le cloud. Les capteurs nous envoient des données télémétriques des environnements d'exécution et nous aident à identifier les écarts de comportement ». Sweet fonctionne selon un modèle SaaS et sera proposé sous la forme d'un abonnement à plusieurs niveaux, le prix dépendant du nombre de fonctionnalités choisies par le client.

Des données de télémétrie d'environnements cibles

Sweet déploie des capteurs d'exécution qui filtrent les données d'application et les traitent dans un cadre interne pour établir le profil des anomalies de comportement de workloads et les contextualiser avec les tactiques, techniques et procédures (TTP) traditionnelles. « Nos capteurs d'exécution nous renvoient la télémétrie de l'environnement cible, y compris les charges de travail, les journaux et les API, et nous aident à établir un comportement de référence pour les applications fonctionnant sur le cloud », a déclaré Eyal Fisher. « Ainsi, en cas d'écart, nous savons qu'il peut s'agir d'une attaque et nous menons une enquête plus approfondie ».

Sweet sera livré sous la forme d'une plateforme modulaire avec une suite différente de fonctionnalités ou de capacités disponibles à chaque niveau de licence. Avec cette annonce, la société a également révélé un financement de démarrage de 12 M$ provenant d'un ensemble de fonds d'investissement et de financeurs providentiels.

Les capteurs utilisent la technologie eBPF

Les capteurs d'exécution de Sweet utilisent la technologie eBPF (extended Berkley Packet Filter), qui permet aux programmes de fonctionner sur des noyaux de systèmes basés sur Linux sans qu'il soit nécessaire d'ajouter des modules supplémentaires ou de modifier le code source du noyau. « La technologie utilisée dans nos capteurs est la technologie eBPF, qui nous permet d'avoir une visibilité au niveau du noyau de chaque nœud de chaque ordinateur, sans qu'il soit nécessaire de l'installer sur l'hôte », a déclaré Eyal Fisher. « Le capteur est donc super léger, super mince et consomme très peu de ressources, mais grâce à la technologie eBPF, nous avons des informations jusqu'à des niveaux granulaires ». La technologie eBPF peut être considérée comme le déploiement d'une machine virtuelle (VM) légère, en bac à sable, au sein du noyau Linux. Elle est généralement considérée comme un moyen de fournir des services tiers, notamment en matière d'observabilité, de sécurité et de réseau.

Article rédigé par
Shweta Sharma, IDG NS (adapté par Célia Seramour)

Une erreur dans l'article?
Proposez-nous une correction