SentinelOne

PRÉSENTATION DE SOLUTION

Intégration des identités à votre stratégie de cybersécurité

Une cybersécurité autonome pour votre infrastructure d'identités

Protection des identités

Face à l'accélération du passage au télétravail et à la migration dans le cloud, le paysage des menaces s'est adapté. Les cybercriminels ciblent les comptes Active Directory et Azure AD des entreprises dans le cadre de cyberattaques visant les identités, afin de s'implanter dans l'environnement convoité. De leur côté, les entreprises abandonnent leur approche de la sécurité axée sur les endpoints et le réseau pour empêcher les cyberpirates d'élargir leur accès, de s'implanter de façon persistante, d'élever leurs privilèges et de se déplacer latéralement.

Les solutions SentinelOne offrent aux entreprises une protection spécifique, avec des fonctionnalités ASM (Attack Surface Management) axées sur les identités et IDTR (Identity Threat Detection & Response). Les solutions ASM axées sur les identités permettent aux équipes de sécurité de réduire la surface d'attaque liée aux identités et de gérer les risques connexes. D'autre part, les solutions ITDR constituent la pierre angulaire d'une stratégie XDR (eXtended Detection and Response) efficace et offrent aux professionnels de la sécurité les informations contextuelles et la visibilité dont ils ont besoin pour prévenir, détecter et neutraliser des menaces telles que le vol et l'utilisation abusive d'identifiants, l'élévation de privilèges et l'exposition des identités.

Avantages de l'ITDR pour les entreprises

Face à l'augmentation du nombre d'attaques ciblant les identités, les entreprises doivent identifier rapidement et efficacement tout exploit, utilisation abusive ou vol d'identifiants d'entreprise. Les cybercriminels utilisent largement des identifiants compromis comme vecteur d'attaque initial, puis exploitent Active Directory (AD) pour développer leurs attaques. Face à la migration des entreprises vers le cloud public et à l'augmentation exponentielle des identités humaines/virtuelles, la protection des identifiants et la détection des attaques ciblant les identités sont devenues des priorités.

Au vu des dommages causés par l'utilisation abusive d'identifiants, il est essentiel d'adopter des solutions qui protègent les surfaces d'attaque axées sur les identités. Les études des analystes montrent que la plupart des compromissions impliquent désormais des identifiants compromis ou détournés, confirmant ainsi que les cybercriminels sont constamment à la recherche d'identifiants valides qu'ils utilisent ensuite pour se déplacer discrètement dans les réseaux. L'utilisation abusive d'identifiants a également contribué à l'essor de menaces telles que le ransomware[1].

L'ITDR : définition et importance

À la base, l'ITDR détecte le vol d'identifiants, l'utilisation abusive ou l'élévation de privilèges, les attaques ciblant Active Directory et les droits d'accès à risques de nature à ouvrir des voies d'attaque. Contrairement aux outils de protection des identités existants (IAM, PAM ou IGA) qui se concentrent sur l'autorisation et l'authentification,

PRINCIPALES FONCTIONNALITÉS

Singularity Identity
étend les fonctionnalités de détection et de réponse de Singularity XDR à vos contrôleurs de domaine Active Directory et Azure AD, ainsi qu'aux endpoints reliés aux domaines afin de les protéger contre les tentatives d'accès, le déplacement latéral et l'exploitation de comptes à privilèges ou d'identifiants.

Singularity Ranger AD
procède à une évaluation continue des erreurs de configuration, des vulnérabilités et des menaces ciblant Active Directory en temps réel, et fournit des conseils pour corriger les expositions et les failles dans les environnements clients AD.

Singularity Hologram
offre un environnement de leurres comprenant des systèmes d'appâts et des données imitant des ressources de production afin de détourner les attaques, d'attirer les cyberattaquants et de collecter des données pour l'investigation numérique afin d'enrichir les renseignements sur les cybercriminels.

1 Verizon, Data Breach Investigations Report