SentinelOne

SCHEDA TECNICA

Singularity™ | IDENTITY

Rilevamento e risposta alle minacce alle identità in tempo reale

AD e Azure AD sono obiettivi comuni degli attacchi informatici basati sulle identità, in quanto la loro compromissione può fornire agli hacker la possibilità di ampliare privilegi e opportunità di accesso, stabilire la persistenza, identificare altri obiettivi e spostarsi lateralmente.

Singularity Identity™, soluzione per il rilevamento e la risposta alle minacce (ITDR) inclusa nella piattaforma SentinelOne Singularity XDR, protegge in tempo reale i controller di dominio di Active Directory e Azure AD e gli endpoint collegati al dominio dagli avversari che cercano di ottenere privilegi e di agire di nascosto. Singularity Identity espande le funzionalità di protezione di Singularity XDR con agenti Sentinel che proteggono i controller di dominio di Microsoft AD e gli endpoint degli utenti finali.

Difendete il vostro dominio

Rilevate gli attacchi ad Active Directory su qualsiasi tipo di dispositivo o sistema operativo, inclusi quelli di tipo IoT e OT, e fornite l'accesso condizionato ad AD tramite soluzioni MFA di terze parti.

Sventate gli attacchi

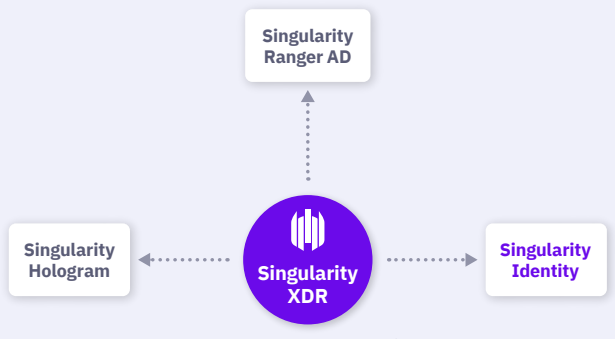
Allontanate gli hacker dai componenti fondamentali di AD e indirizzateli verso vicoli ciechi.

Nascondete, deviate, proteggete

Nascondete le credenziali e i dati di produzione rendendo al contempo difficile il movimento laterale.

Estendete la portata con l'integrazione

Eseguite l'integrazione con le esche della rete di Singularity Hologram™ per rallentare ulteriormente gli avversari e le minacce interne sulla rete.



Componenti dell'identità

Singularity Identity Sentinels impedisce agli hacker di accedere ai componenti cruciali di Active Directory e Azure AD, sia on-premise che nel cloud

Per maggiori informazioni, visitate **s1.ai/identity**

L'**84%** delle organizzazioni ha subito una violazione delle identità. Singularity Identity Sentinels protegge le identità in tempo reale.

FUNZIONALITÀ E VANTAGGI PRINCIPALI

+ Rilevamento in tempo reale degli attacchi informatici alle identità basati su Active Directory e Azure AD, incluso il ransomware
+ Facile implementazione con risultati a basso impatto; supporta Active Directory on-premise, Azure AD e ambienti multi-cloud
+ Copertura degli attacchi alle identità e massima sicurezza per tutte le risorse gestite e non gestite su tutti i sistemi operativi, compresi quelli dei dispositivi IoT e OT
+ Tecnologia di cloaking per ingannare gli hacker e proteggere le credenziali ad elevato valore
+ Informazioni utili sulle falle nella superficie di attacco associata alle identità, quali errori di configurazione, controlli degli accessi insufficienti, violazioni dei criteri e altro ancora
+ Si integra con la tecnologia di inganno di Singularity Hologram per l'interazione tramite esche sulla rete e la raccolta di informazioni sulle minacce

Tenete le credenziali al sicuro, generate valore rapidamente

Iniziate presto a sfruttare i vantaggi della nostra soluzione con opzioni di implementazione rapide, flessibili e prive di complicazioni: Singularity Identity offre la copertura completa per AD on-premise, Azure AD e ambienti multi-cloud. Rafforzate immediatamente le vostre difese proteggendo e limitando l'accesso agli archivi di credenziali delle applicazioni locali, identificando le esposizioni delle identità e implementando controlli in grado di sventare gli attacchi.

Funzionalità di Singularity Identity

01 | Difendete le identità nel controller di dominio

L'agente Sentinel di Singularity Identity per AD e Azure AD rileva gli attacchi basati sulle identità nell'intera infrastruttura del dominio. Singularity Identity fornisce informazioni utili e altamente affidabili nel momento in cui gli attacchi vengono rilevati sui dispositivi gestiti e non gestiti potenzialmente compromessi, compresi quelli IoT e OT più diffusi, indipendentemente dal sistema operativo o dall'ubicazione. L'agente Sentinel fornisce inoltre l'accesso condizionato ad AD tramite integrazioni con soluzioni MFA di terze parti.

02 | Difendete l'identità sull'endpoint

L'agente Sentinel di Singularity Identity per endpoint rileva l'utilizzo improprio delle identità e le attività di ricognizione che avvengono nell'ambito dei processi relativi agli endpoint e che prendono di mira server di dominio critici, account di servizio, credenziali locali e dati locali, di rete e nel cloud. Le tecniche di cloaking e inganno integrate nell'agente rallentano l'avversario, assicurandovi al contempo la situational awareness.

03 | Bloccate il movimento laterale

Bloccate l'avanzamento degli avversari, inclusi gli attacchi ransomware, con trappole disseminate ovunque: Singularity Identity vi consente di prevenire il furto delle credenziali con privilegi, incluse quelle ad elevato valore degli account di utenti, servizi e sistemi. Le attività non autorizzate di ricognizione e rilevamento delle impronte digitali sulla rete vengono rese praticamente inutili per gli hacker, poiché i dati reali vengono sostituiti da dati esca. Inoltre, grazie all'integrazione con Singularity Hologram, potete anche reindirizzare i tentativi di movimento laterale verso esche sulla rete.

04 | Scoprite i percorsi di attacco

Singularity Identity vi aiuta a scoprire e a comprendere gli elementi nascosti che rendono il vostro ambiente suscettibile agli attacchi basati sulle identità, come le superfici esposte, le credenziali orfane e le violazioni dei criteri. Singularity Identity include mappe topografiche visive che mostrano come gli hacker potrebbero spostarsi all'interno dei sistemi per raggiungere le risorse critiche. Grazie a queste informazioni, i vostri team di sicurezza e IT possono bloccare in via preventiva i percorsi verso le risorse critiche e rafforzare le difese utilizzando la tecnologia di inganno.

ADOZIONE DI UN MODELLO ZERO TRUST CON SINGULARITY IDENTITY

+ Considerate implicitamente attendibili solo le applicazioni e le risorse di dati
+ Identificate le esposizioni di identità su endpoint, AD e cloud
+ Rilevate gli attacchi alle identità sferrati da endpoint e controller di dominio
+ Limitate l'accesso alle sole applicazioni attendibili o convalidate
+ Consente l'accesso condizionato ad AD tramite soluzioni MFA di terze parti

Singularity Identity si integra con Singularity Hologram™ per offrire una soluzione completa di inganno e protezione delle identità.

ULTERIORI INFORMAZIONI

Visitate **s1.ai/identity**

Informazioni su SentinelOne

SentinelOne (NYSE:S) è all'avanguardia nella sicurezza informatica automatizzata e previene, rileva e risponde agli attacchi informatici in modo più rapido e preciso che mai. La nostra piattaforma Singularity XDR protegge e supporta le aziende leader a livello mondiale offrendo loro visibilità in tempo reale sulle superfici di attacco, correlazione tra piattaforme e risposte basate sull'intelligenza artificiale. Ottenete più funzionalità e meno complessità.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733