SentinelOne

FICHE TECHNIQUE

Singularity | IDENTITY

Une solution ITDR pour la protection en temps réel des identités

Active Directory et Azure AD sont des cibles fréquentes de cyberattaques axées sur les identités. Et pour cause : leur compromission permet aux attaquants de se positionner dans l'environnement de manière à élargir leur accès, s'implanter de façon persistante, élever leurs privilèges, identifier d'autres cibles et se déplacer latéralement.

Singularity Identity™ est une solution ITDR (Identity Threat Detection and Response) qui s'intègre à la plateforme SentinelOne Singularity XDR. Grâce à des agents déployés sur les machines, elle protège en temps réel les contrôleurs de domaine Microsoft Active Directory (AD) et Azure AD ainsi que les endpoints reliés aux domaines contre les utilisations abusives de privilèges et les déplacements latéraux des cybercriminels.

Protection de votre domaine

Détectez les attaques ciblant Active Directory, quels que soient le type d'équipement ou le système d'exploitation dont elles émanent (y compris les systèmes IoT et OT), et accordez un accès conditionnel à Active Directory grâce aux solutions MFA partenaires.

Mise en échec des cybercriminels

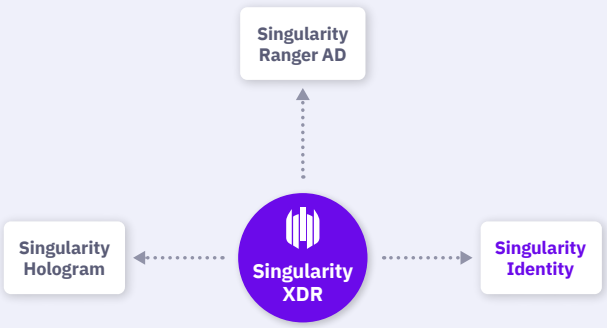
Détournez les cybercriminels des informations critiques stockées dans l'Active Directory et redirigez-les vers des voies sans issue.

Dissimulation, esquive et protection

Faites obstacle au déplacement latéral des attaquants, et soustrayez les identifiants et les données de production à leur vue.

Extension de la protection et collecte d'informations

Intégrez Singularity Identity à la technologie de leurres réseau de Singularity Hologram™ pour mieux freiner les cybercriminels infiltrés dans le réseau et les acteurs malveillants internes.



Composants de la solution ITDR

Les agents SentinelOne de Singularity Identity empêchent les attaquants d'accéder aux informations critiques stockées dans l'Active Directory et d'Azure AD, qu'elles soient hébergées sur site ou dans le cloud.

Pour plus informations, consultez **s1.ai/identity**

84 % des entreprises ont été victimes d'une compromission liée aux identités. Les agents SentinelOne de Singularity Identity protègent les identités en temps réel.

PRINCIPAUX AVANTAGES ET FONCTIONNALITÉS

+ Détection en temps réel des cyberattaques contre les identités qui ciblent Active Directory et Azure AD, y compris les ransomwares
+ Implémentation simplifiée sans nuire à l'efficacité opérationnelle ; prise en charge d'Active Directory local, d'Azure AD et des environnements multicloud
+ Protection contre les attaques ciblant les identités : couverture complète pour toutes les ressources gérées et non gérées, quel que soit le système d'exploitation, y compris pour les équipements IoT et OT
+ Technologie de dissimulation conçue pour induire en erreur les attaquants et protéger les identifiants critiques
+ Informations exploitables sur les failles présentes au niveau des identités, notamment les problèmes de configuration, les contrôles d'accès inappropriés, les violations de stratégie, etc.
+ Intégration de la solution à la technologie de leurres de Singularity Hologram pour la configuration de leurres réseau et la collecte de cyberveille sur les menaces

Sécurisation des identifiants et retour sur investissement plus rapide

Tirez rapidement parti de la solution grâce à un déploiement flexible, simple et sans impact sur l'efficacité opérationnelle : Singularity Identity offre une couverture de protection complète pour l'Active Directory local, Azure AD et les environnements multicloud. Améliorez immédiatement votre système de défense en protégeant et en limitant l'accès aux référentiels d'identifiants des applications locales, en identifiant les expositions des identités et en appliquant des contrôles qui déjouent les attaques.

Fonctionnalités de Singularity Identity

01 | Protection des identités au niveau du contrôleur de domaine

L'agent SentinelOne de Singularity Identity pour Active Directory et Azure AD détecte les attaques ciblant les identités à partir de n'importe quel élément composant l'infrastructure du domaine. Singularity Identity fournit des informations exploitables facilement lorsque des équipements gérés ou non gérés, y compris les systèmes IoT et OT, sont victimes d'attaques et risquent d'être compromis, quel que soit leur système d'exploitation ou leur emplacement. En outre, l'agent SentinelOne permet de définir un accès conditionnel à Active Directory grâce à des intégrations avec des solutions tierces de MFA.

02 | Protection des identités au niveau de l'endpoint

L'agent SentinelOne pour endpoint de Singularity Identity détecte les activités de reconnaissance et d'exploitation d'identités survenant dans des processus sur l'endpoint exécutés pour atteindre des cibles critiques : serveurs de domaine, comptes de service, identifiants locaux, données locales, données réseau ou données cloud. Les techniques de leurres et de dissimulation on-agent ralentissent le cybercriminel tout en conférant aux équipes une connaissance approfondie de la situation.

03 | Blocage des déplacements latéraux

Arrêtez la progression des cybercriminels et des attaques, y compris des ransomwares, grâce à des pièges et des leurres placés de manière pertinente. Singularity Identity vous permet d'empêcher le vol d'identifiants à privilèges, notamment ceux des comptes système, des comptes de service et des comptes utilisateur critiques. Les activités non autorisées de reconnaissance réseau et d'identification par empreinte ne sont plus d'aucune utilité pour les attaquants, car les données légitimes sont remplacées par des données fictives. En intégrant la solution à Singularity Hologram, vous pourrez également rediriger les tentatives de déplacement latéral vers des leurres réseau.

04 | Identification des chemins empruntés par les attaques

Singularity Identity vous aide à découvrir et à comprendre les causes cachées de la vulnérabilité de votre environnement aux attaques ciblant les identités, comme les surfaces exposées, les identifiants orphelins et les violations de stratégie. Grâce notamment à des cartes topographiques visuelles, la solution vous montre comment les attaquants sont parvenus à se déplacer d'un système à l'autre pour atteindre les ressources critiques. Fortes de ces informations, vos équipes de sécurité et IT sont à même d'agir de manière préventive en bloquant les voies d'accès aux ressources critiques et en renforçant vos défenses à l'aide de la technologie de leurres.

ADOPTER ET APPLIQUER LE ZERO TRUST AVEC SINGULARITY IDENTITY

+ Limitez la confiance implicite pour l'accès aux applications et données.
+ Identifiez l'exposition des identités au niveau des endpoints, d'Active Directory et du cloud.
+ Détectez les attaques ciblant les identités sur les endpoints et sur les contrôleurs de domaine.
+ Limitez l'accès aux seules applications approuvées ou validées.
+ Activez l'accès conditionnel à Active Directory en intégrant des solutions MFA de fournisseurs partenaires.

Singularity Identity s'intègre à Singularity Hologram™ pour vous offrir une solution complète combinant technologie de leurres et protection des identités.

POUR EN SAVOIR PLUS

Consultez **s1.ai/identity**

À propos de SentinelOne

SentinelOne (NYSE : S) propose une cybersécurité autonome de pointe, capable de prévenir, détecter et neutraliser les cyberattaques plus rapidement et plus précisément que jamais. Sa plateforme Singularity XDR protège les grandes entreprises mondiales en leur offrant visibilité en temps réel sur les surfaces d'attaque, corrélation entre plateformes et réponse aux incidents optimisée par l'intelligence artificielle. Vous disposez ainsi de plus de fonctionnalités, tout en réduisant la complexité de votre écosystème de sécurité.

fr.sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733