SentinelOne

LÖSUNGSÜBERSICHT

Integration von Identität in die Cybersicherheitsstrategie

Autonome Cybersicherheit für Ihre Identitätsinfrastruktur

Identitätssicherheit

Mit dem schnellen Umstieg zur Remote-Arbeit in der Cloud hat sich auch die Bedrohungslandschaft verändert. Die Angreifer nehmen nun das lokale Active Directory und Azure AD-Konten mit identitätsbasierten Cyberattacken ins Visier, um sich in einer Umgebung festzusetzen. Als Reaktion darauf wenden sich Unternehmen vom Geräte- und Netzwerk-orientierten Sicherheitsmodell ab, um die Angreifer davon abzuhalten, ihren Zugang zu erweitern, Persistenz zu erzielen, Zugriffsrechte auszuweiten oder sich lateral zu bewegen.

Die umfassenden Lösungen von SentinelOne unterstützen Unternehmen mit Funktionen für Identitätsschutz, die extra für diesen Zweck entwickelt wurden und Umgebungen mithilfe einer identitätsorientierten Angriffsflächenverwaltung (Attack Surface Management, ASM) sowie Erkennung von und Reaktion auf Identitätsbedrohungen (Identity Threat Detection and Response, ITDR) schützen. Während identitätsorientierte ASM-Lösungen dazu dienen, identitätsbasierte Angriffsflächen zu verringern und deren Risiken zu verwalten, fungiert ITDR als Grundstein einer effektiven XDR-Strategie (Extended Detection and Response). Das Sicherheitsteam erhält den Kontext und Überblick, den es zur Prävention, Erkennung und Abwehr von Bedrohungen wie Diebstahl und Missbrauch von Anmeldedaten, Rechteausweitung und Identitätskompromittierungen benötigt.

Warum ITDR für Unternehmen wichtig ist

Identitätsbasierte Angriffe nehmen zu. Deshalb müssen Unternehmen heute schnell und effektiv erkennen, wenn Angreifer ihre Anmeldedaten ausnutzen, missbrauchen oder stehlen. Immer häufiger werden kompromittierte Anmeldedaten als Erstangriffsvektor genutzt und der Angriff anschließend über das Active Directory (AD) ausgeweitet. Durch den Wechsel in die Public Cloud und die enorm wachsende Anzahl menschlicher bzw. maschineller Identitäten werden der Schutz von Anmeldedaten und die Erkennung identitätsbasierter Angriffsaktivitäten immer wichtiger.

Angesichts der Schäden durch den Missbrauch von Identitäten müssen Unternehmen Lösungen einsetzen, die identitätsbasierte Angriffsflächen schützen können. Wie Untersuchungen von Analysten gezeigt haben, spielen bei den meisten aktuellen Zwischenfällen kompromittierte Anmeldedaten eine Rolle. Das ist auch der Grund dafür, warum Angreifer immer wieder gültige Anmeldedaten erbeuten und dazu nutzen wollen, sich unerkannt im Netzwerk zu bewegen. Zudem ermöglicht der Missbrauch von Anmeldedaten auch Taktiken wie Ransomware[1].

Was ist ITDR und warum ist es wichtig?

Die Hauptfunktion von ITDR ist die Erkennung von Anmeldedatendiebstahl, Erweiterung oder Missbrauch von Privilegien, Angriffen auf das Active Directory und gefährlichen Berechtigungen, die potenzielle Angriffswege bieten. Im Gegensatz zu bestehenden Identitätsschutztools wie IAM, PAM oder IGA, bei denen Autorisierung

1 Verizon: Data Breach Investigations Report

WICHTIGE FUNKTIONEN

Singularity Identity
erweitert die Erkennungs- und Reaktionsfunktionen von Singularity XDR auf das Active Directory und die Azure AD-Domänen-Controller sowie mit der Domäne verbundene Endpunkte und schützt diese vor Angreifern, die privilegierte Konten oder Anmeldedaten missbrauchen und sich unbemerkt bewegen wollen.

Singularity Ranger AD
bewertet Konfigurationsfehler, Schwachstellen und aktive Bedrohungen für das AD kontinuierlich sowie in Echtzeit und gibt Anleitungen zum Schließen von Schwachstellen und Lücken in den AD-Umgebungen der Kunden.

Singularity Hologram
bietet eine vorgetäuschte Umgebung mit Ködersystemen und Daten, die Assets in der Produktionsumgebung nachahmen, um Angriffe fehlzuleiten, Angreifer auf sich zu ziehen und forensische Daten über Angreifermethoden zu sammeln.

und Authentifizierung im Fokus stehen, bieten ITDR-Lösungen dem Sicherheitsteam die Transparenz und den Schutz, den Identitätsverwaltungssysteme benötigen. Eine ausgereifte ITDR-Lösung kann identitätsbasierte Angriffe erkennen und nutzt dabei Kontext, um den Missbrauch von Anmeldedaten und Versuche von Rechteausweitung oder laterale Bewegungen zu identifizieren. Diese Lösungen bieten nicht nur Schutzmaßnahmen auf Domänen-Controller-Ebene, sondern können zudem Anmeldedaten schützen, die auf Endpunkten gespeichert sind. Dazu verbirgt ITDR die Daten vor den Angreifern und hindert nicht autorisierte Prozesse daran, auf den Anmeldedatenspeicher von Anwendungen zuzugreifen.

Ebenso wie andere Erkennungs- und Reaktionslösungen bieten ITDR-Lösungen den Unternehmen Transparenz und autonome Reaktionsfunktionen sowie Fehlleitung und Täuschung. Wenn eine Lösung einen identitätsbasierten Angriff erkennt, kann sie zum Beispiel gefälschte Daten bereitstellen, die die Angreifer zu einem für das System unwichtigen Köder weiterleiten. Zudem kann die Lösung das kompromittierte System, auf dem der identitätsbasierte Angriff stattfindet, automatisch vom Rest des Netzwerks isolieren und seine Aktivitäten damit auf die Köderumgebung beschränken.

Was ist identitätsorientierte Angriffsflächenverwaltung?

Die identitätsorientierte Angriffsflächenverwaltung arbeitet mit der ITDR-Lösung zusammen, um Unternehmen einen Überblick über AD-Konfigurationsfehler, auf Endpunkten gespeicherte Anmeldedaten und andere Probleme zu geben, die ein Unternehmen anfällig machen könnten. Durch die verringerte Angriffsfläche kann das Sicherheitsteam seine Abwehr stärken und die vertraulichen Daten sowie die Infrastruktur effektiv schützen.

Wenn Angreifer einen Endpunkt kompromittiert haben, schicken sie Abfragen an das AD, um ungeschützte Objekte, Konten und Privilegien ausfindig zu machen, mit denen sie ihren Angriff ausbauen können. Sie durchsuchen die AD-Controller nach Schwachstellen, über die sie sich lateral bewegen und privilegierten Zugriff oder die Kontrolle über die Domäne erlangen können. Mit identitätsorientierten ASM-Lösungen erhalten Sie Einblicke in Probleme der AD-Sicherheitshygiene sowie verwertbare Warnungen zu Schwachstellen auf Domänen-, Rechner- und Benutzerebene. Die Lösung kann AD-Angriffsindikatoren in Echtzeit erkennen und durchsucht das AD nach Informationen, ohne die Geschäftsabläufe zu beeinträchtigen. Zudem überwacht sie kontinuierlich die Risiken privilegierter Konten in Bezug auf Anmeldedaten, Dienstkonten, inaktive Konten, gemeinsam genutzte Anmeldedaten und identitätsbasierte Angriffswege.

Die Identitätssicherheitslösungen von SentinelOne

SentinelOne unterstützt das Sicherheitsteam im Unternehmen bei der Entwicklung autonomer und robuster Cybersicherheits-Frameworks für identitätsbasierte Angriffsflächen.

Unser Portfolio an Identitätssicherheitslösungen basiert auf unserer Erfahrung bei der Erkennung von Rechteausweitung und lateralen Bewegungen und macht uns zu einem führenden Anbieter auf dem Markt für ITDR- und identitätsorientierte ASM-Lösungen. Im vergangenen Jahr haben wir aufgrund unseres Portfolios an ITDR- und identitätsbasierten ASM-Lösungen unsere Führungsposition festigen können.

Zusammenfassung

Mit den Identitätssicherheitslösungen von SentinelOne verfügen Sicherheitsexperten über die richtigen Werkzeuge, um die neuesten Cybersicherheitsbedrohungen zu neutralisieren. Sie erhalten damit die nötigen Erkennungs- und Reaktionsfunktionen, um identitätsbasierte Angriffe zu erkennen, ihre Sicherheitsumgebung an die neuesten Best Practices anzupassen und Transparenzlücken in den vorhandenen Sicherheitstechnologien zu schließen.

Informationen zu SentinelOne

SentinelOne (NYSE:S) ist ein Vorreiter auf dem Gebiet der autonomen Cybersicherheit und verhindert, erkennt und stoppt Cyberangriffe schneller und genauer als je zuvor. Unsere Singularity XDR-Plattform schützt und stärkt weltweit führende Unternehmen mit einem Echtzeitüberblick über Angriffsflächen sowie mit plattformübergreifender Korrelation und KI-gestützten Reaktionen. Nutzen Sie mehr Optionen mit geringerer Komplexität.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733