SentinelOne

Singularity | IDENTITY

Checkliste zu Identitätssicherheit

Da Bedrohungsakteure immer häufiger identitätsbasierte Angriffsflächen ins Visier nehmen, entscheiden sich immer mehr Unternehmen für Identitätssicherheitslösungen, die Funktionen zur Prävention, Erkennung und Abwehr bieten. Damit können Indikatoren für den Diebstahl oder Missbrauch von Anmeldedaten, übermäßige Berechtigungen und Angriffe, die auf Rechteausweitung und lateraler Bewegung basieren, erkannt und neutralisiert werden.

Mithilfe dieser Checkliste können CISOs die Risiken in Bezug auf Identität und Berechtigungen erkennen und aufdecken, die in ihren Umgebungen, auf Endpunkten und Netzwerken sowie im Active Directory und in Cloud-basierten Oberflächen oder Assets lauern.

Überblick über Schwachstellen und Risiken

- Wie erhält Ihr Sicherheitsteam einen Überblick über identitätsbezogene Risiken (z. B. Risiken in Bezug auf Anmeldedaten, Berechtigungen, Privilegien)?
- Wie bewertet Ihr Team diese Risiken auf den Endpunkten, im Active Directory und in der Cloud?
- Wie viel Aufwand ist für die Identifizierung der identitätsbezogenen Risiken nötig?
- Wie viel Überblick haben Sie über Angriffswege im Rahmen der Angriffsflächenverwaltung?
- Welchen Grad an Transparenz bieten Ihnen Ihre Identitätssicherheitslösungen auf Benutzer-, Gerät- und Domänenebene?
- Welche Probleme in Bezug auf Konten, Richtlinien, Gruppen, Infrastrukturen, Kerberos-Sicherheit, gefährliche Delegierungen oder andere Probleme können Ihre Lösungen erkennen?
- Wie oft werden diese Risiken neu bewertet?
- Wie werden die Risiken nachverfolgt?
- Wie werden die Ergebnisse und die Risiken in Verbindung mit diesen Ergebnissen visualisiert?
- Wie oft werden diese Informationen aktualisiert?

Angriffserkennung

- Wie erkennen Sie identitätsbasierte Angriffe auf Endpunkten, im Active Directory und in der Cloud?
- Wie groß ist der manuelle Aufwand für die Erkennung identitätsbasierter Angriffe?
- Wie schnell kann Ihr Sicherheitsteam identitätsbasierte Angriffe erkennen und abwehren?
- In welchem Umfang werden Daten von verschiedenen Sicherheitslösungen zur Erkennung identitätsbasierter Angriffe gemeinsam genutzt?
- Wie begegnen Sie identitätsbasierten Angriffen im Zusammenhang mit lateraler Bewegung, Diebstahl von Anmeldedaten oder Rechteausweitung?

Behebung und Beseitigung

- Welche Behebungsoptionen bieten Ihre Sicherheitslösungen?
- Welches Maß an Automatisierung bieten Ihre Tools zur Behebung?
- Welche Informationen zur Beseitigung bietet die Lösung, wenn keine Behebung möglich ist?

Analyse

- Wie verwertbar sind die Warnungen Ihrer Lösung? Ordnet der Anbieter Erkennungen dem MITRE ATT&CK-Framework oder einem anderen Sicherheits-Framework zu?
- Wie stellt die Identitätssicherheitslösung ihre Ergebnisse dar?
- Welche Analysetools bietet die Lösung? In welchem Umfang können Daten von anderen Lösungen genutzt werden?

Wenn CISOs die Stärken und Schwächen ihrer vorhandenen Identitätssicherheitslösungen kennen, können sie die Eignung der Funktionen von Mitbewerberprodukten besser einschätzen. Wir empfehlen den Sicherheitsteams, zu berücksichtigen, welchen Umfang an Transparenz und Erkennung eine Lösung bietet. Zudem sollten Sie darauf achten, ob die Lösung eine umfassende Abdeckung von den Endpunkten über das Active Directory bis hin zu Multi-Cloud-Umgebungen bietet.

Innovativ. Vertrauenswürdig. Anerkannt.

Gartner

Führender Anbieter im 2021 Magic Quadrant für Endpoint Protection-Plattformen

MITRE ENGENUITY

Rekordergebnis bei der ATT&CK-Bewertung

- 100 % Schutz. 100 % Erkennung.
- Höchste analytische Abdeckung 3 Jahre in Folge
- 100 % Echtzeit und keinerlei Verzögerungen

Gartner peerinsights. 4,9

99 % der Gartner Peer Insights™

EDR-Analysten empfehlen SentinelOne Singularity

FedRAMP · AICPA SOC · TEVORA PCI DSS Attestation HIPAA Attestation · VB 100 VIRUS · AAA · SE Labs BEST Innovator WINNER 2021

Informationen zu SentinelOne

SentinelOne ist Vorreiter auf dem Gebiet der autonomen Cybersicherheit und verhindert, erkennt und stoppt Cyberangriffe schneller, umfangreicher und genauer, als das mit ausschließlich manuellen Technologien möglich ist. Die Singularity XDR-Plattform bietet Ihnen Echtzeit-Transparenz und intelligente KI-gestützte Reaktion. Nutzen Sie mehr Optionen mit geringerer Komplexität.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733