DATENBLATT

Starling Identity Analytics & Risk Intelligence

Nützliche Informationen – effektive Nutzung von Sicherheitsdaten

Vorteile

- Sicherheits-Intelligence: beschleunigt die Ermittlung von problematischen Zugriffsberechtigungen und Verstößen zur Verbesserung der allgemeinen Sicherheit
- Verwaltete Transparenz: sorgt für einen besseren Überblick über potenzielle Risikofaktoren oder Schwachstellen für eine bessere Priorisierung von Nachforschungen
- Analysen: verbessert die Risikoerkennung und die Analysegenauigkeit für eine bessere Fokussierung von Abhilfemaßnahmen
- Entlastung: mindert den administrativen Aufwand, da Berechtigungsdaten nicht mehr manuell erfasst und verarbeitet werden müssen
- Gesamtbetriebskosten: verbessert die Effizienz und Effektivität und senkt die Gesamtbetriebskosten

Beim Thema Sicherheit gibt es keinen Stillstand. In der Vergangenheit diente Identity and Access Management (IAM, Identitäts- und Zugriffsverwaltung) vor allen Dingen dem Schutz des Unternehmens. Heutzutage muss es allerdings auch die digitale Transformation von Organisationen unterstützen. Setzen Sie IAM endlich richtig um – mit einer Identity as a Service (IDaaS)-Lösung, mit der sich die Risiken für solche Unternehmensinitiativen reduzieren lassen. Unterstützen Sie die digitale Transformation Ihrer Organisation mit einer Lösung, die Ihnen eine schnelle Erkennung von Bedrohungen und eine effiziente Untersuchung von abweichendem Verhalten ermöglicht, sodass Sie leicht Entscheidungen treffen, Aktionen priorisieren und Risiken beheben können.

Mithilfe von Starling Identity Analytics & Risk Intelligence (IARI) reduzieren Sie Risiken und somit auch Ihre Angriffsfläche, bevor Bedrohungen sich auf Ihren Betrieb auswirken. Dies gelingt Ihnen durch die Aufhebung von unnötigen oder inaktiven Berechtigungen, die andernfalls missbräuchlich oder unsachgemäß verwendet werden könnten. Starling IARI zeigt Ihnen Risiken und Zugriffsvorgänge auf, sodass Sie Sicherheitsentscheidungen deutlich schneller treffen können.

ONE IDENTITY™

Nützliche Informationen, mit denen Sie feststellen können:

- Ob eine Person tatsächlich alle ihre Berechtigungen nutzt
- Ob die gewährten Berechtigungen für die Rolle eines Benutzers angemessen sind
- Ob ein Benutzer mit umfassenden Berechtigungen diese überhaupt haben sollte
- Wie die Berechtigungen eines Benutzers im Vergleich zu denen seiner Kollegen, zum Rest der Organisation oder sogar im Vergleich zu anderen Organisationen aussehen
- Warum einBenutzer zunächst wenige Berechtigungen hatte und anschließend über mehr verfügt

Starling Identity Analytics & Risk Intelligence – die wichtigsten Funktionen

Datenquellenmodule und Collector

Automatisiert die Erfassung, Verarbeitung und Übertragung von Berechtigungsdaten aus Zieldatenquellen und ermöglicht ein schnelles Hinzufügen von Datenquellen.

Risikoklassifizierungsregeln

Erfasst und verarbeitet gewährte Berechtigungen in Gruppen und Klassifizierungen. Auf diese Weise wird eine Berechtigungsübersicht bereitgestellt, über die sich Berechtigungen mit hohem Risikopotenzial identifizieren lassen.

Benutzerrisikoprofile

Gleicht gewährte Berechtigungen mit Risikoklassifizierungsregeln ab, sodass Konten mit hohem Risikopotenzial identifiziert werden können. Bei Änderungen an dem Risikoprofil eines Kontos wird eine Benachrichtigung ausgegeben und die Änderungen können mithilfe einer Unternehmensverifizierung weitergehend validiert werden.

Benachrichtigung und Unternehmensverifizierung

Gibt eine Benachrichtigung aus, wenn gewährte Berechtigungen und die daraus resultierenden Änderungen am Benutzerrisikoprofil in den Bereich für hohes Risikopotenzial abrutschen. Der Inhaber des Profils kann dann die Rollenzertifizierungen mit Blick auf Sicherheitsbedrohungen überprüfen und analysieren, die Auswirkungen auf das Geschäft haben.

Berechtigungsnutzungsanalysen

Identifiziert inaktive Zugriffsberechtigungen und initiiert Governance- und/oder Abhilfemaßnahmen.

Zugriffsvergleichund Peer Group-Analyse

Vergleicht Benutzer und Peer Groups innerhalb der Organisation und über diese hinaus. Dadurch können Populationen ähnlicher Benutzer mit vergleichbaren Berechtigungen identifiziert und Unterschiede lokalisiert werden, sodass sich eine Priorisierung im Hinblick auf die Behebung von zugriffsbezogenen Problemen vornehmen lässt.

Analyse-Dashboards und Berichte

Compliance- und Betriebs-Dashboards, Berichte zur Benutzeridentität sowie Zugriffs- und Auditdaten ermöglichen einen direkten Überblick, sodass Bemühungen von IT-Mitarbeitern, Unternehmensbenutzern und Auditoren besser priorisiert werden können.

Eine Testversion und Informationen zu den neuesten Aktualisierungen im Hinblick auf Produktfunktionen finden Sie unter One Identity Starling.

Infos über One Identity

Die One Identity Lösungen für Identity and Access Management bieten IAM für den Praxiseinsatz und umfassen geschäftsorientierte, modulare, integrierte und zukunftsfähige Lösungen für Identity Governance, Zugriffsverwaltung und Verwaltung privilegierter Konten.

Weitere Informationen: OneIdentity.com

Datasheet-StarlingAnalytics&Risk-US-CW-DE-WL-30120

ONE IDENTITY™