Überwachung von Malwarerisiken in AWS S3 und Azure Storage mit Cloud-Malware

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Malware-Risiken in AWS S3 und Azure Storage mit Cloud-Malware überwacht und behoben werden.

Überblick

Mit dieser Funktion können Sie Malware-Risiken in Ihren AWS S3- und Azure Storage-Umgebungen erkennen und überwachen. Ein wichtiger Anwendungsfall besteht darin, mit Malware infizierte Dateien zu identifizieren, die Anmeldeinformationen stehlen oder Schwachstellen ausnutzen können, wodurch das Risiko einer lateralen Verschiebung innerhalb Ihrer Umgebung oder in andere Umgebungen steigt.

Unterstützte Reaktionsaktionen für AWS und Azure

Derzeit wird nur die Überwachung als Reaktionsaktion für AWS S3 und Azure Storage unterstützt. Automatische Wiederherstellungsaktionen, wie das Löschen oder Quarantäne von Dateien, sind nicht verfügbar. Diese Einschränkung verhindert versehentliche Unterbrechungen geschäftskritischer Services und ermöglicht Ihnen dennoch die Überwachung auf vertrauliche Daten und Malware-Risiken.

Zugehörige Ressourcen

- Cloud-Malware-Schutz für AWS-Tenants aktivieren
- Cloud-Malware-Schutz für Azure-Tenants aktivieren

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.