Monitoraggio dei rischi di malware in AWS S3 e nell'archiviazione di Azure con malware cloud

Sommario

Introduzione

In questo documento viene descritto come monitorare e risolvere i rischi di malware in AWS S3 e nell'archiviazione di Azure con malware cloud.

Panoramica

Grazie a questa funzionalità è ora possibile individuare e monitorare i rischi di malware negli ambienti AWS S3 e di archiviazione di Azure. Uno scenario chiave consiste nell'identificazione di file infetti da malware in grado di rubare credenziali o sfruttare vulnerabilità, aumentando il rischio di spostamento laterale all'interno dell'ambiente o in altri ambienti.

Azioni di risposta supportate per AWS e Azure

Attualmente, solo il monitoraggio è supportato come azione di risposta per AWS S3 e Archiviazione di Azure. Non sono disponibili azioni di monitoraggio e aggiornamento automatici, ad esempio l'eliminazione o la quarantena dei file. Questa limitazione impedisce l'interruzione accidentale dei servizi mission-critical e consente di monitorare l'esposizione dei dati sensibili e i rischi di malware.

Risorse correlate

- Abilita protezione malware cloud per tenant AWS
- Abilita Cloud Malware Protection per tenant di Azure

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).