Malwarerisico's in AWS S3 en Azure Storage bewaken met cloudmalware

Inhoud

Inleiding

In dit document wordt beschreven hoe u malwarerisico's in AWS S3 en Azure Storage met cloudmalware kunt bewaken en aanpakken.

Overzicht

Met deze functie kunt u nu malware-risico's in uw AWS S3- en Azure Storage-omgevingen detecteren en bewaken. Een belangrijke use case is het identificeren van bestanden die zijn geïnfecteerd met malware die inloggegevens kunnen stelen of kwetsbaarheden kunnen misbruiken, waardoor het risico op zijwaartse beweging in uw omgeving of naar andere omgevingen toeneemt.

Ondersteunde responsacties voor AWS en Azure

Momenteel wordt alleen bewaking ondersteund als een responsactie voor AWS S3 en Azure Storage. Automatische herstelacties, zoals het verwijderen van bestanden of quarantaine, zijn niet beschikbaar. Deze beperking voorkomt onbedoelde onderbreking van bedrijfskritieke services, terwijl u toch kunt controleren op blootstelling aan gevoelige gegevens en malwarerisico's.

Gerelateerde bronnen

- Cloud Malware Protection voor AWS-huurders inschakelen
- Cloud Malware Protection voor Azure-huurders inschakelen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.