为S3存储段的HTTPS事务配置日志查询字符串参数

目录

简介

本文档介绍要记录到s3存储桶的HTTPS事务的新日志查询参数。

概述

现在提供新的日志记录功能，支持将完整HTTPS请求（包括查询字符串参数）记录到s3存储桶。

默认情况下，在将详细信息记录到Umbrella的报告和S3存储段之前，Umbrella会从所有HTTPS请求中删除查询字符串参数。这样做是为了防止无意中暴露任何报告中的查询参数，因为它们可能包含私人或敏感信息。

s3存储桶通常用于向SIEM和专家报告工具提供活动数据。通过为HTTPS事务启用日志查询参数，这些工具可以更深入地了解HTTPS请求。

1. HTTPS流量（加密）、查询字符串参数继续从Umbrella报告控制面板中删除。
2. 对于HTTP流量（非加密），Umbrella始终记录包括查询字符串参数的完整URL。HTTP流量的参数不视为“敏感”，因为应用/网站不对其进行加密。

有关如何启用此新的s3存储桶日志记录功能的更多详细信息，请参阅Umbrella文档。

- 启用记录到您自己的S3存储桶 — https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-your-own-s3-bucket
- 启用登录到思科管理的S3存储桶 — https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-a-cisco-managed-s3-bucket

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。