Configure Log Query String Parameters for HTTPS Transactions to S3 Buckets

Contents

Introduction

This document describes new log query parameters for HTTPS transactions to be logged to an s3 bucket.

Overview

A new logging capability is now available that enables the full HTTPS request including the query string parameters to be logged to an s3 bucket.

By default, Umbrella strips the query string parameters from all HTTPS requests before logging the details to Umbrella's reporting and S3 bucket. This is done to prevent inadvertently exposing the query parameters in any reports because they can potentially contain private or sensitive information.

The s3 bucket is often used to provide activity data to SIEM and specialist reporting tools. By enabling the Log query parameters for HTTPS transactions these tools can gain more visibility and insight into the HTTPS requests.

1. The HTTPS traffic (encrypted), the query string parameters continue to be removed from the Umbrella reporting dashboard.
2. For HTTP traffic (non-encrypted), Umbrella has always logged the Full URL including the query string parameters. The parameters for HTTP traffic are not deemed to be 'sensitive' because the app/website does not encrypt them.

For more details on how to enable this new s3 bucket logging capability, please refer to the Umbrella documentation.

- Enable Logging to Your Own S3 Bucket - https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-your-own-s3-bucket

- Enable Logging to a Cisco-managed S3 Bucket - https://docs.umbrella.com/umbrella-user-guide/docs/enable-logging-to-a-cisco-managed-s3-bucket