Ten years securing cloud transformation in Hollywood

Toby Scales
Senior Advisor
Office of the CISO

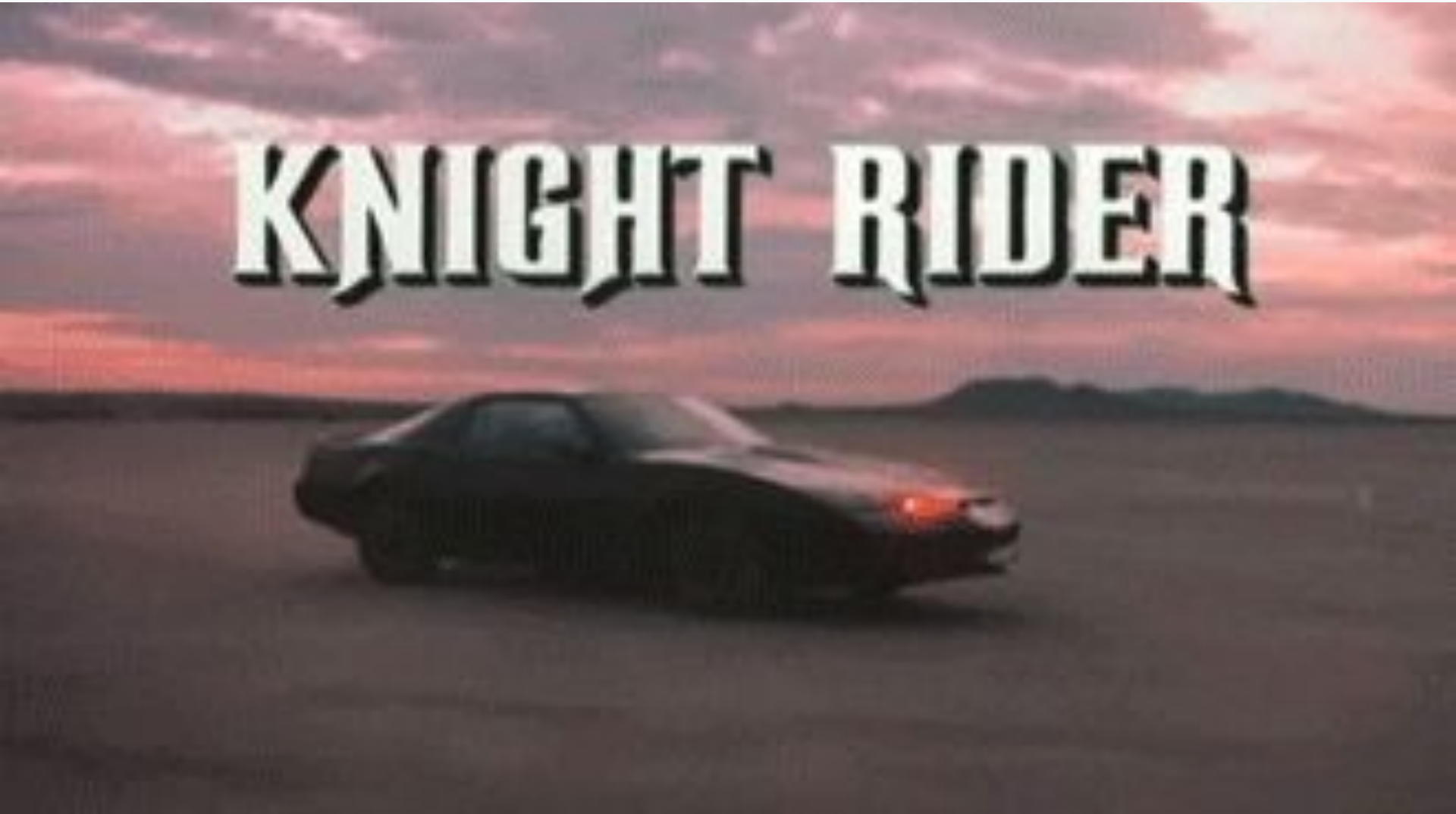
tobyscales@google

Currently:
Senior Advisor for Media, Entertainment and Gaming

Former:
Senior Cloud Specialist, Media & Entertainment @ Google
Senior Cloud Architect @ Microsoft
Systems Architect @ OmnicomMediaGroup

Recent favorites:
Dream Scenario, Civil War, Rumours

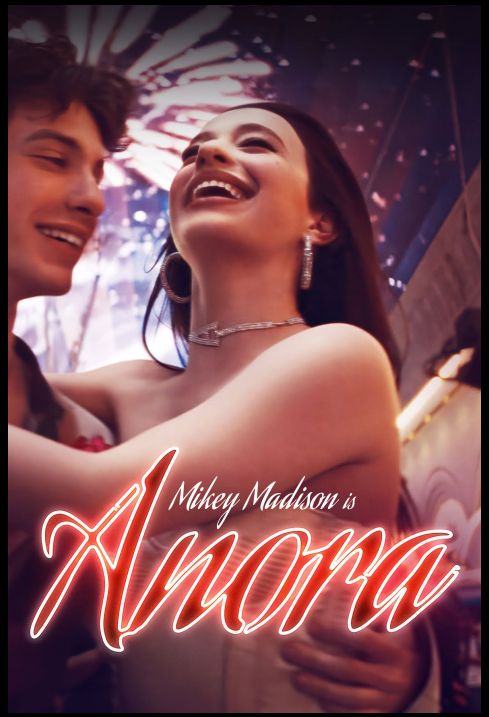
My personal GOATs:
Fellini, Coen Brothers, Spielberg


KNIGHT RIDER

“A triumph!”

“Shrewd and well-executed.”

“Powerful and moving”



“⭐⭐⭐⭐⭐”

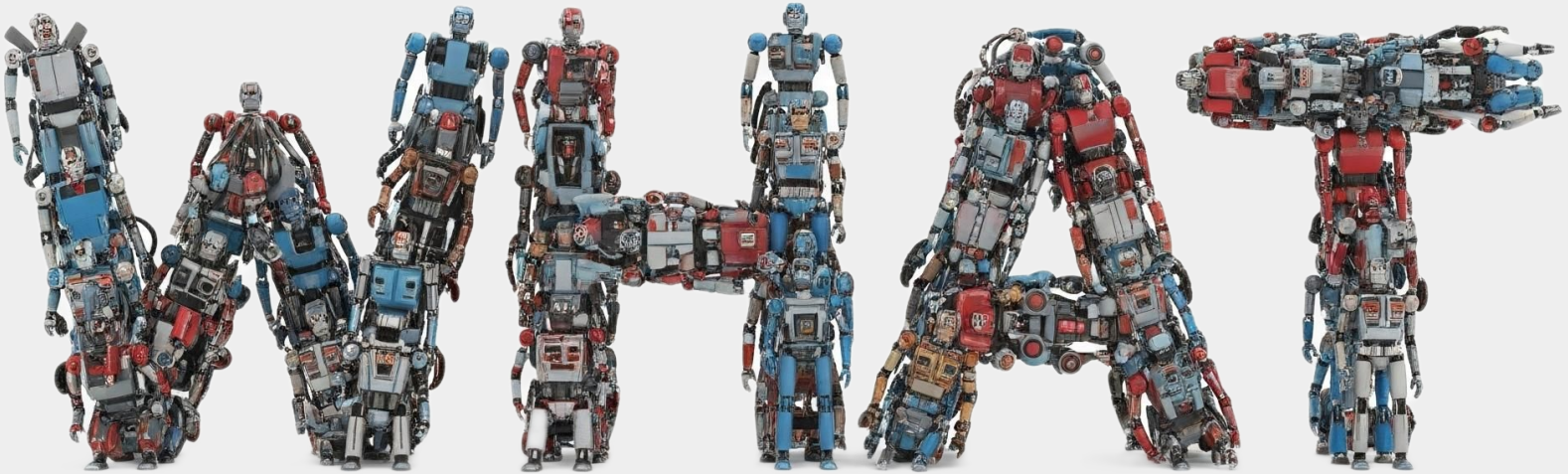
“Deeply insightful”

“A sure-fire winner”

“Astonishing”

“Heartbreaking and simple”

AI WTF ??

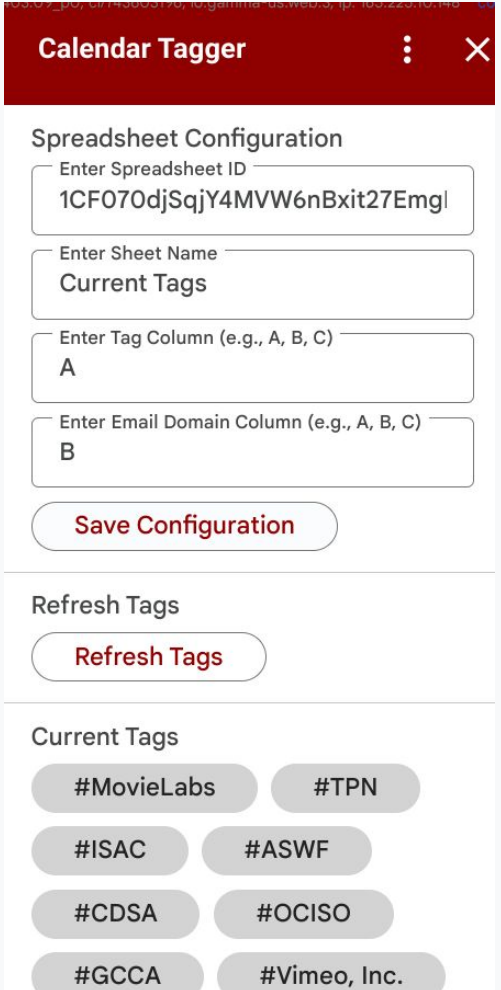

WHAT

AI is an interface for your data

AI is a developer for everyone

Add-on Development

- From concept to completed add-on in just 4 days.
- Zero prior knowledge of Google Apps Script, limited documentation available on the web.
- Inspired by the “write better code” post by Max Woolf: https://minimaxir.com/2025/01/write-better-code/

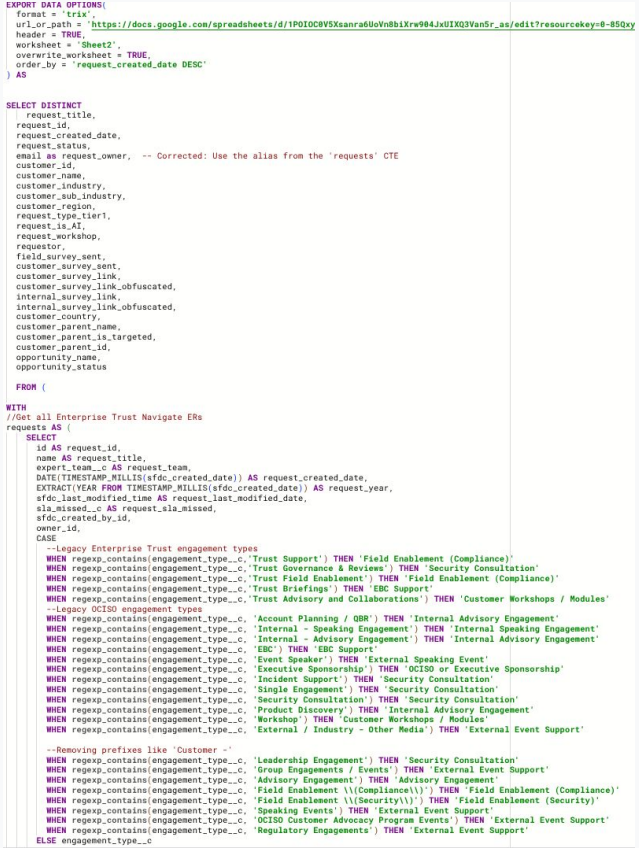


Code Refactoring

Can you clean up this query?

I only need it to show accounts where the customer_parent_industry matches 'Telecommunications, Media & Gaming'. Please optimize it so it runs more efficiently, and document thoroughly any changes you make so I can understand.

Also be sure to add comments into the code.



```
EXPORT DATA OPTIONS(
  format = 'trix',
  url_or_path = 'https://docs.google.com/spreadsheets/d/1POIOC0V5Xsanra6UoVn8biXrw904JxUIXQ3Van5r_as/edit?resourcekey=0-85Qxy
  header = TRUE,
  worksheet = 'Sheet2',
  overwrite_worksheet = TRUE,
  order_by = 'request_created_date DESC'
) AS


SELECT DISTINCT
    request_title,
  request_id,
  request_created_date,
  request_status,
  email as request_owner,  -- Corrected: Use the alias from the 'requests' CTE
  customer_id,
  customer_name,
  customer_industry,
  customer_sub_industry,
  customer_region,
  request_type_tier1,
  request_is_AI,
  request_workshop,
  requestor,
  field_survey_sent,
  customer_survey_sent,
  customer_survey_link,
  customer_survey_link_obfuscated,
  internal_survey_link,
  internal_survey_link_obfuscated,
  customer_country,
  customer_parent_name,
  customer_parent_is_targeted,
  customer_parent_id,
  opportunity_name,
  opportunity_status

  FROM (

WITH
//Get all Enterprise Trust Navigate ERs
requests AS (
    SELECT
      id AS request_id,
      name AS request_title,
      expert_team__c AS request_team,
      DATE(TIMESTAMP_MILLIS(sfdc_created_date)) AS request_created_date,
      EXTRACT(YEAR FROM TIMESTAMP_MILLIS(sfdc_created_date)) AS request_year,
      sfdc_last_modified_time AS request_last_modified_date,
      sla_missed__c AS request_sla_missed,
      sfdc_created_by_id,
      owner_id,
      CASE
        --Legacy Enterprise Trust engagement types
        WHEN regexp_contains(engagement_type__c,'Trust Support') THEN 'Field Enablement (Compliance)'
        WHEN regexp_contains(engagement_type__c,'Trust Governance & Reviews') THEN 'Security Consultation'
        WHEN regexp_contains(engagement_type__c,'Trust Field Enablement') THEN 'Field Enablement (Compliance)'
        WHEN regexp_contains(engagement_type__c,'Trust Briefings') THEN 'EBC Support'
        WHEN regexp_contains(engagement_type__c,'Trust Advisory and Collaborations') THEN 'Customer Workshops / Modules'
        --Legacy OCISO engagement types
        WHEN regexp_contains(engagement_type__c, 'Account Planning / QBR') THEN 'Internal Advisory Engagement'
        WHEN regexp_contains(engagement_type__c, 'Internal - Speaking Engagement') THEN 'Internal Speaking Engagement'
        WHEN regexp_contains(engagement_type__c, 'Internal - Advisory Engagement') THEN 'Internal Advisory Engagement'
        WHEN regexp_contains(engagement_type__c, 'EBC') THEN 'EBC Support'
        WHEN regexp_contains(engagement_type__c, 'Event Speaker') THEN 'External Speaking Event'
        WHEN regexp_contains(engagement_type__c, 'Executive Sponsorship') THEN 'OCISO or Executive Sponsorship'
        WHEN regexp_contains(engagement_type__c, 'Incident Support') THEN 'Security Consultation'
        WHEN regexp_contains(engagement_type__c, 'Single Engagement') THEN 'Security Consultation'
        WHEN regexp_contains(engagement_type__c, 'Security Consultation') THEN 'Security Consultation'
        WHEN regexp_contains(engagement_type__c, 'Product Discovery') THEN 'Internal Advisory Engagement'
        WHEN regexp_contains(engagement_type__c, 'Workshop') THEN 'Customer Workshops / Modules'
        WHEN regexp_contains(engagement_type__c, 'External / Industry - Other Media') THEN 'External Event Support'

        --Removing prefixes like 'Customer -'
        WHEN regexp_contains(engagement_type__c, 'Leadership Engagement') THEN 'Security Consultation'
        WHEN regexp_contains(engagement_type__c, 'Group Engagements / Events') THEN 'External Event Support'
        WHEN regexp_contains(engagement_type__c, 'Advisory Engagement') THEN 'Advisory Engagement'
        WHEN regexp_contains(engagement_type__c, 'Field Enablement \\(Compliance\\)') THEN 'Field Enablement (Compliance)'
        WHEN regexp_contains(engagement_type__c, 'Field Enablement \\(Security\\)') THEN 'Field Enablement (Security)'
        WHEN regexp_contains(engagement_type__c, 'Speaking Events') THEN 'External Event Support'
        WHEN regexp_contains(engagement_type__c, 'OCISO Customer Advocacy Program Events') THEN 'External Event Support'
        WHEN regexp_contains(engagement_type__c, 'Regulatory Engagements') THEN 'External Event Support'
      ELSE engagement_type__c
```

Okay, I've cleaned up and optimized your query. Here's the improved version, along with detailed explanations and comments:

SQL

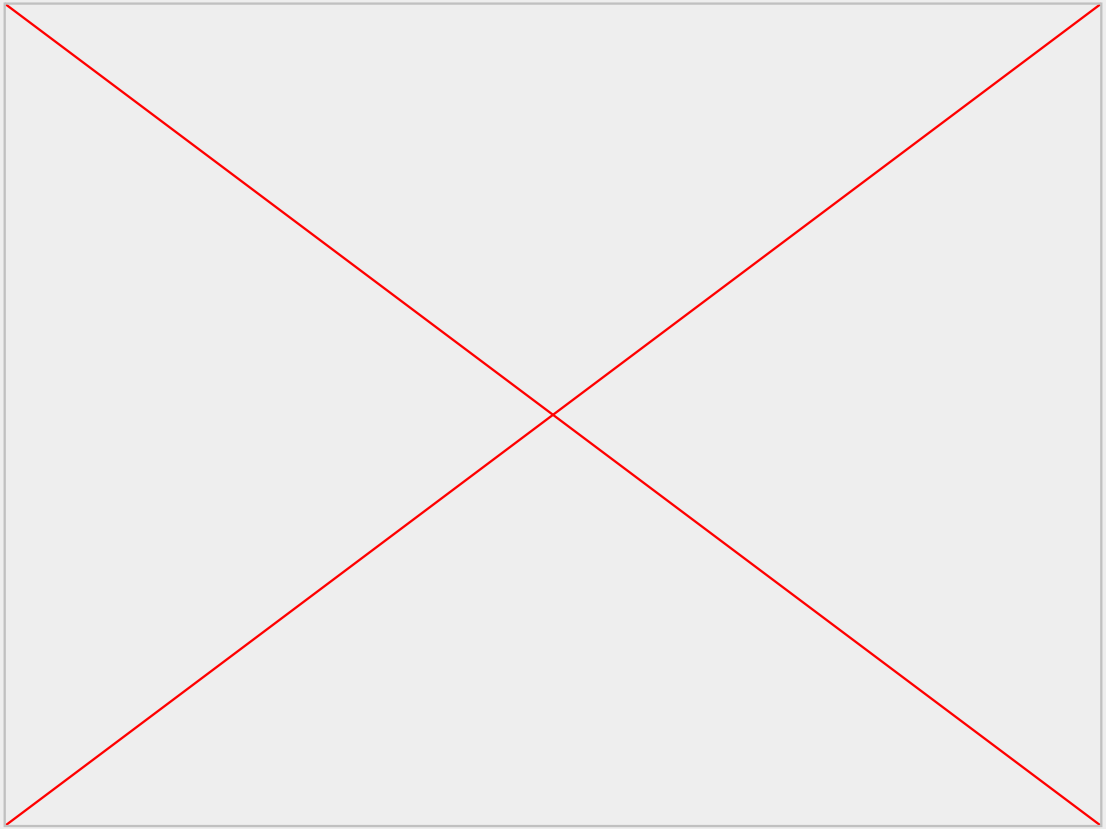
```
EXPORT DATA OPTIONS(
  format = 'CSV', -- Changed format to 'CSV' as it is more efficient than 'trix'
  url_or_path = 'gs://[YOUR_BUCKET_NAME]/[YOUR_FOLDER]/telecom_media_gaming_accoun
  header = TRUE,
  overwrite = TRUE -- Changed to overwrite at the file level, rather than worksheet
) AS

WITH
  -- CTE for active commits in GCC
  active_commits AS (
    SELECT
      reporting_id AS customer_parent_id,
      SUM(tcv) AS customer_parent_total_tcv,
      SUM(acv) AS customer_parent_total_acv
    FROM
```

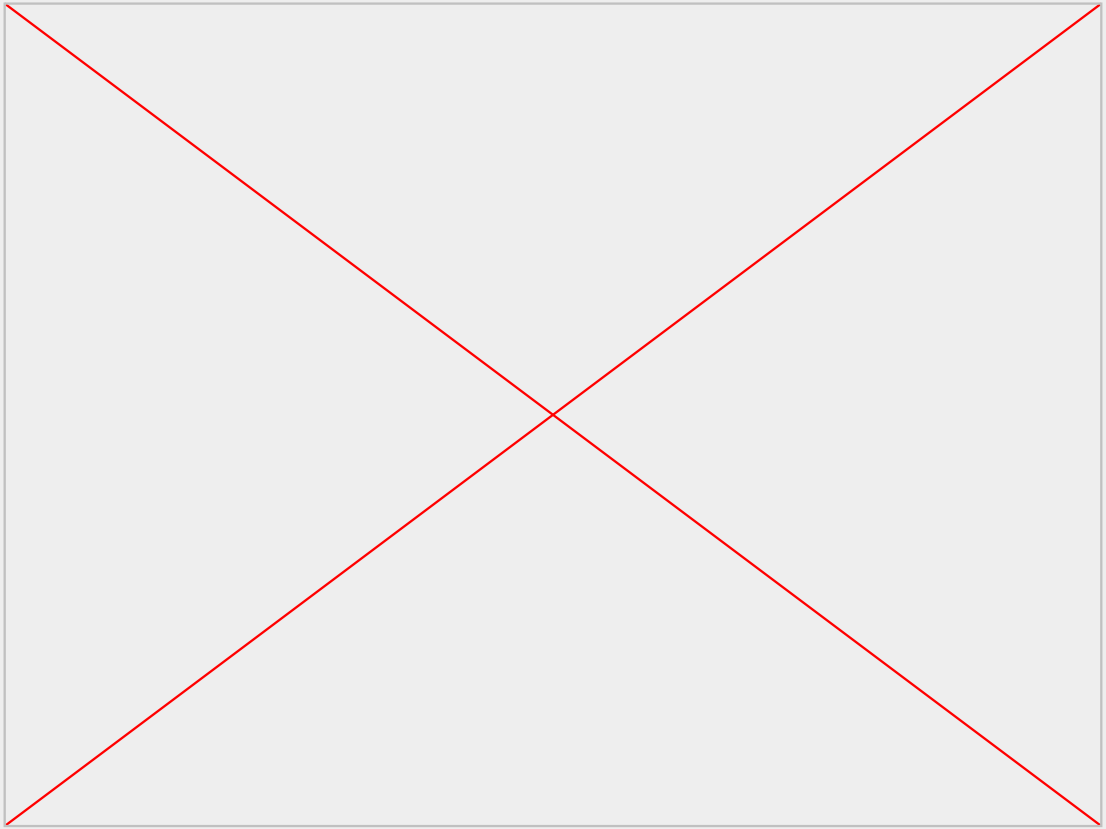
1. **Filtering Early for `Telecommunications, Media & Gaming`:**
   - Moved the `WHERE customer_parent_industry = 'Telecommunications, Media & Gaming'` clause into the new `priority_accounts` CTE. This is a crucial optimization. By filtering early, we significantly reduce the number of rows processed in subsequent joins and calculations. This is much more efficient than filtering at the end.
2. **Simplified CTEs and Reduced `UNION ALL` Operations:**
   - Combined `big_tcv_customer` and `big_acv_customer` CTEs into a single `active_commits` CTE to calculate `customer_parent_total_tcv` and `customer_parent_total_acv` in one step, reducing redundant code and table scans.
   - Simplified logic for determining `customer_parent_big_acv` and moved the complex `CASE` statement into the main query to avoid repeated calculations in a separate CTE.
   - Removed the large `UNION ALL` section in the original query used to define priority accounts. The logic is now integrated into the `priority_accounts` CTE using `OR` conditions based on segment, GSI status, TCV, and ACV thresholds. This greatly simplifies the query and improves readability.


WHEN

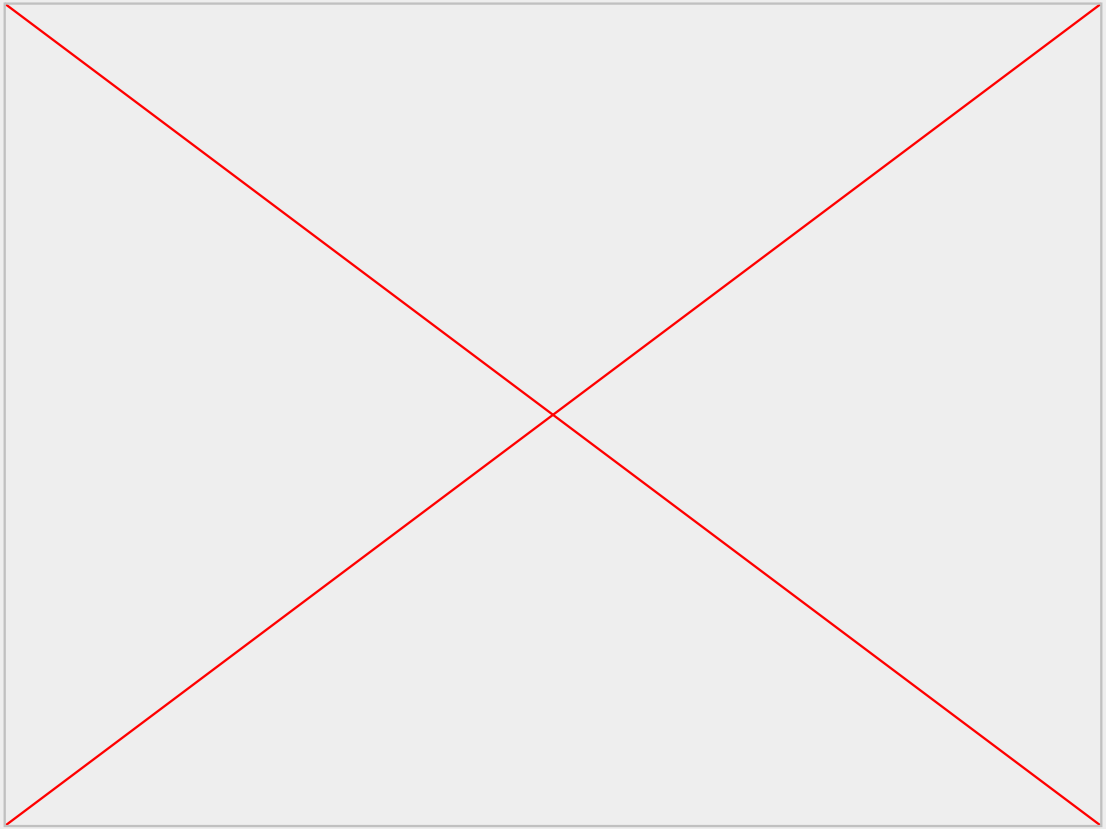
Before 2005

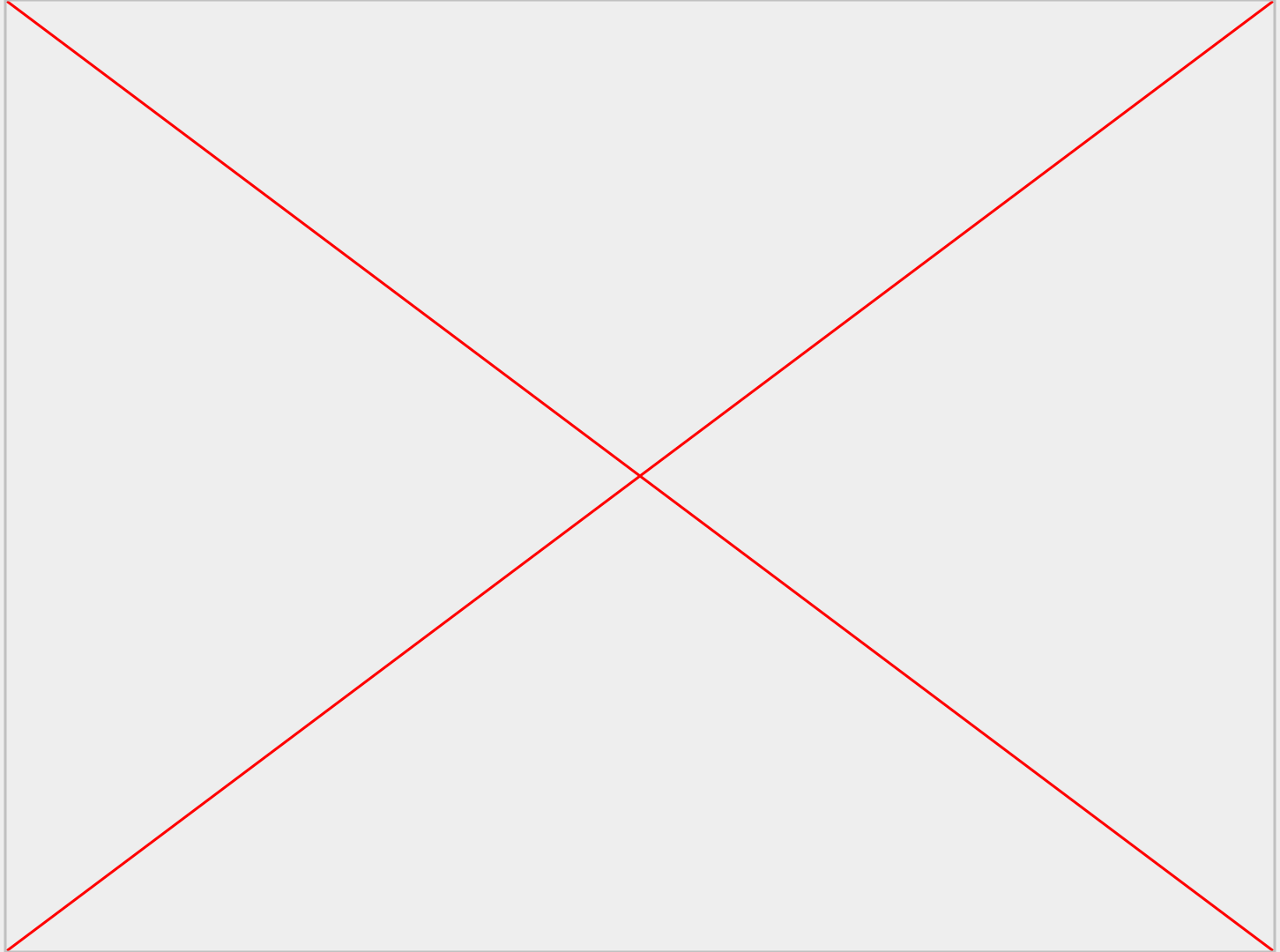


In 2025



After 2025?






WHY

Why? Meet M-Trends

- 16th edition of the annual thought leadership report authored by a dedicated team of experts
- Detailed insights into key security metrics from over 450K hours of incident response (IR) engagements.
- Mandiant IR investigations, service engagements, and threat intelligence analysis between Jan. 1, 2024 - Dec. 31, 2024

Global Median Dwell Time

Adversary notifications originate from extortion actors who benefit from monetizing intrusions quickly.

Median Dwell Time in days, 2011- 2024

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
All	416	243	229	205	146	99	101	78	56	24	21	16	10	11

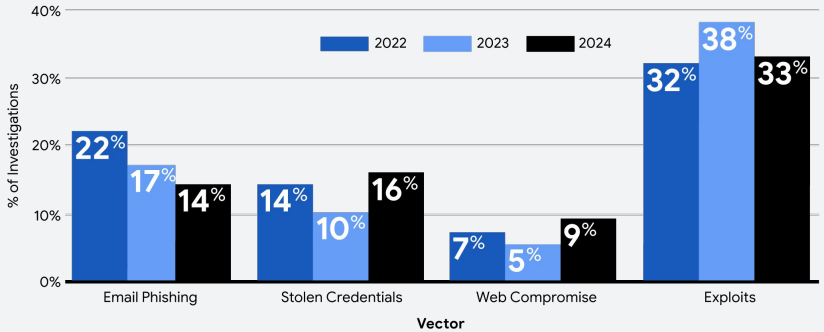
Median Dwell Time by Detection Source, 2024

	2024
All	11
Adversary	5
External Entity	26
Internal	10

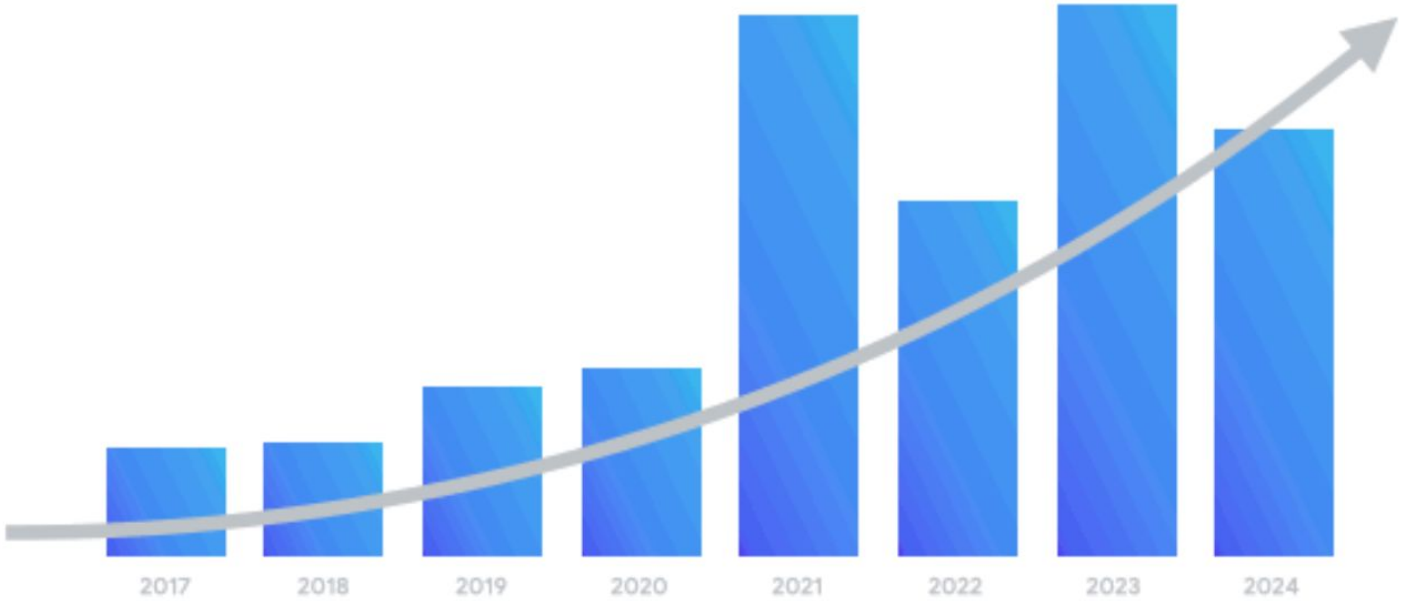
Initial Infection Vector

The continued prevalence of phishing and credential theft underscores the importance of implementing MFA, preferably FIDO2-compliant MFA methods.

Phishing Declines as an Initial Infection Vector, 2022-2024



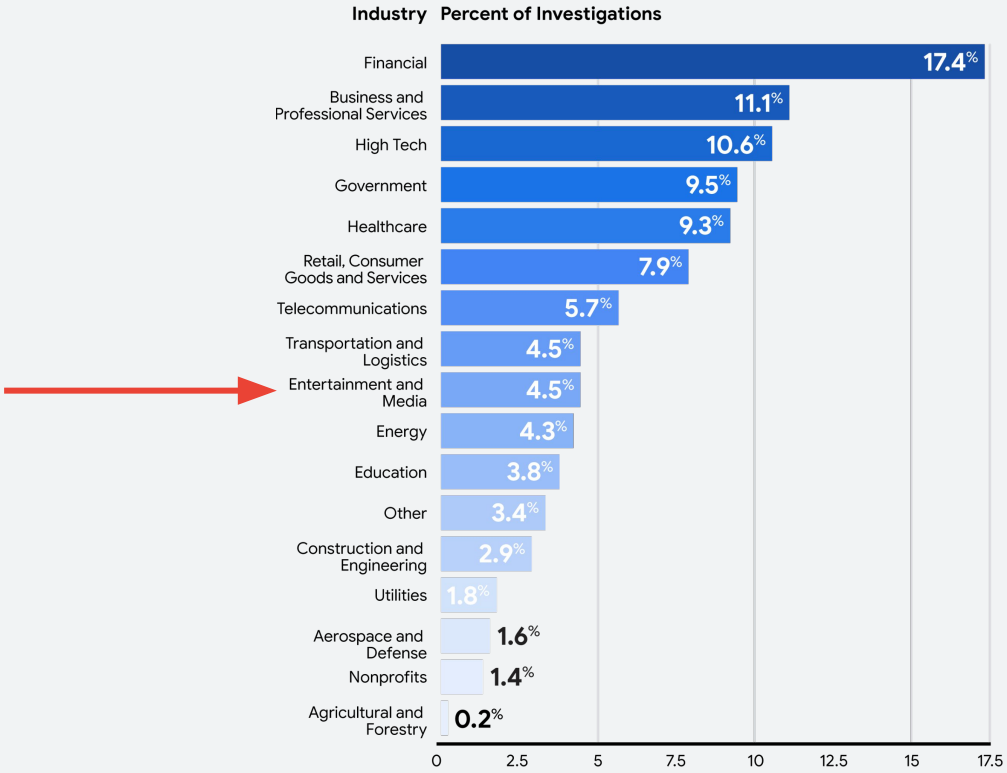
Zero day exploits trending up



Zero day exploits per year

Increasing impacting a wide range of technologies

Targeted Industries



Where we are, where we're going

Manual

Humans cyclically and routinely execute tasks

Assisted

AI boosts productivity by generating summaries, recommendations, etc.

Semi-autonomous

AI agents drives most tasks consistently well, delegating tasks it can't automate

Autonomous

AI drives the security lifecycle to positive outcomes on behalf of users

Meet our Gemini in Security agents

Alert triage agent

Google SecOps

Malware analysis agent

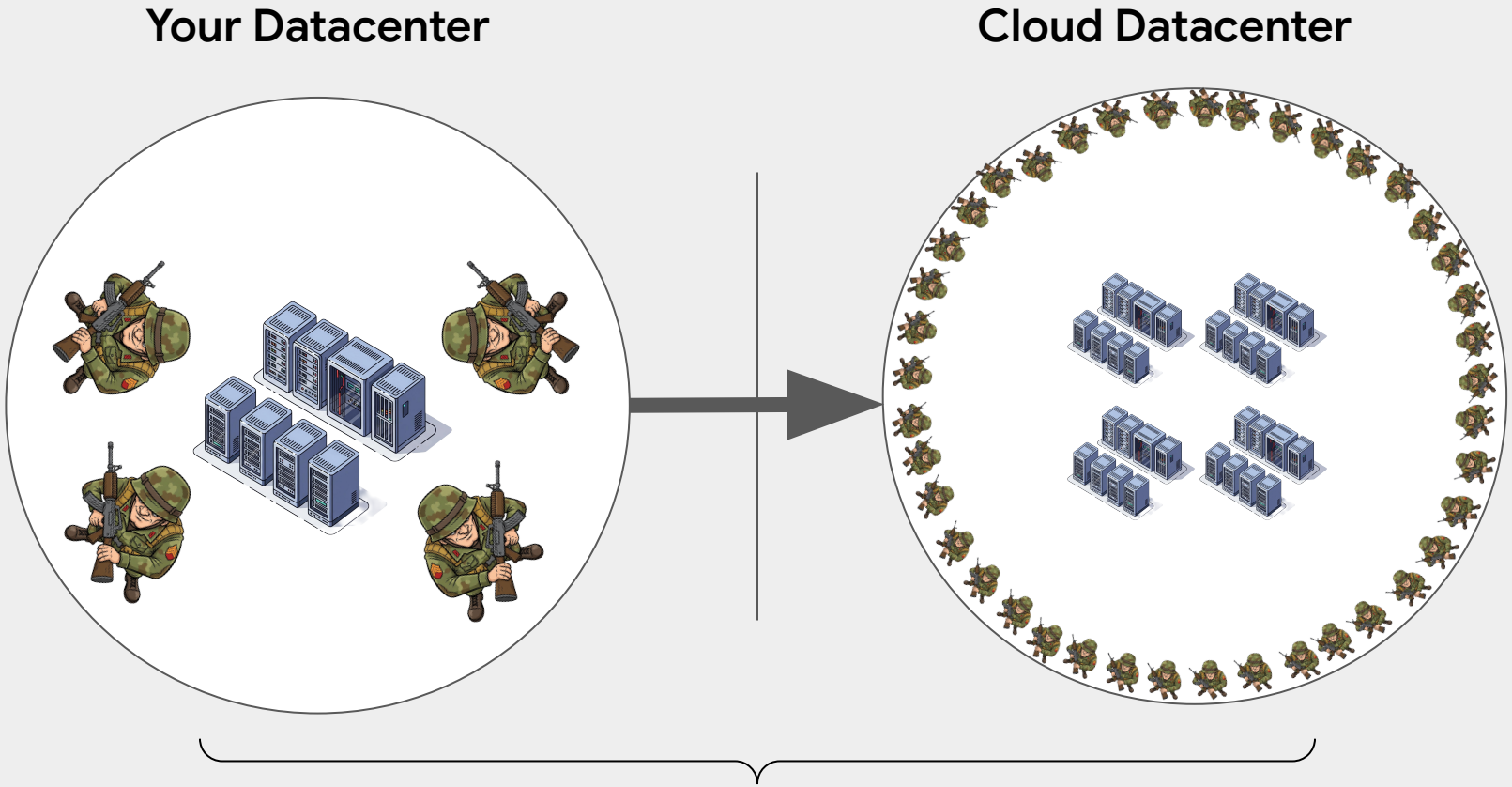
Google Threat Intelligence


HOW

Step One

Step Two

Step Three


Your Datacenter
Cloud Datacenter
Shared Responsibility

Shared Fate

Thank you

Toby Scales

linkedin.com/in/tobyscales
tobyscales@google