KUSTO DETECTIVE AGENCY 2

powered by AMD

Recruiting now at

detective.kusto.io

KUSTO DETECTIVE AGENCY

powered by AMOJI

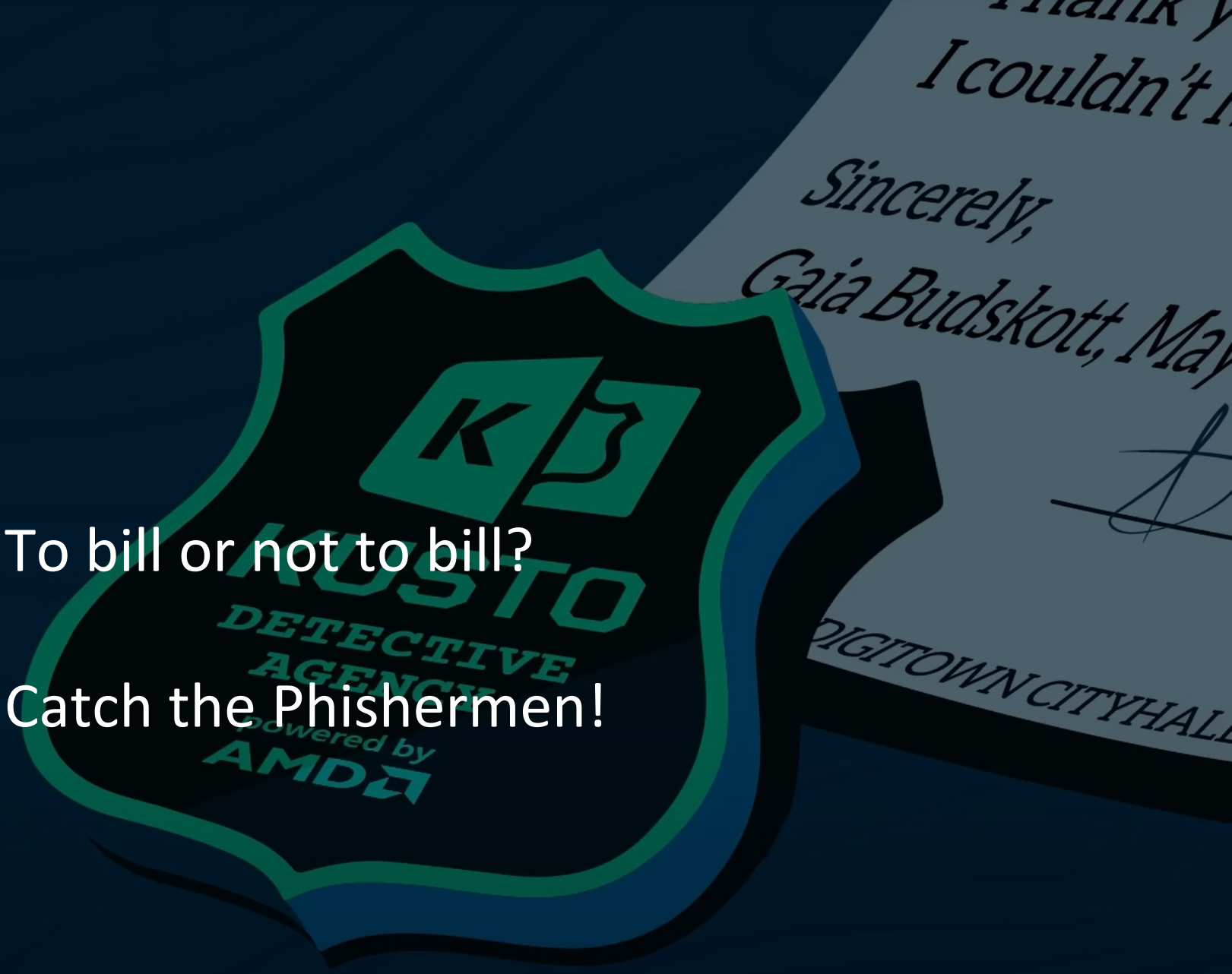
JOIN THE KUSTO DETECTIVE AGENCY

You may open Microsoft Fabric KQL database
or Azure Data Explorer free cluster

Application Insights

Agenda

1. Onboarding
2. Solving Case 1 – To bill or not to bill?
3. Solving Case 2 – Catch the Phishermen!



Rules of the game

Work together! It’s more fun to share your progress and ask for help.

There are a total of 15 cases (10 for Season 2, 5 for Season 1).

A digital badge is given to every player who correctly solves a case.

All previous cases will remain active for play even after the new cases are published.

Please see section 6 in the “Terms and Conditions” for more details.

Walkthrough Demo – Please follow along!

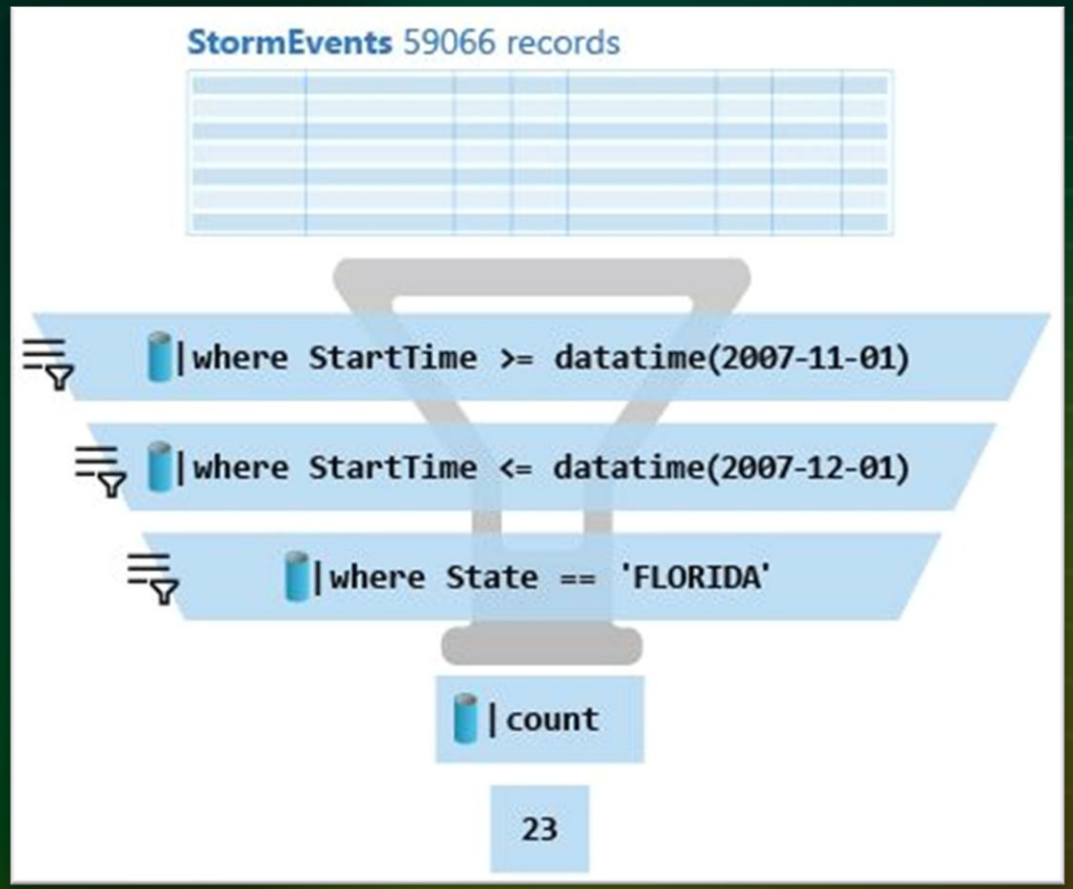
1. ADX Web-UI / KE tool
2. Sample Queries – write it with us!

Kusto Query Language (KQL)

- A powerful query language to explore data in ADX to find **patterns**, **trends**, identify **anomalies**, perform **exploratory** and **observational** analytics.
- A Kusto query is a read-only request on data with filters and aggregates that work in a **top-down approach**

For Example

```
StormEvents
| where StartTime between (datetime(2007-11-01) .. datetime(2007-12-01))
| where State == "FLORIDA"
| count
```



KQL Basic Operators

```
… | count
```

- Counts records in input table (e.g. T)

```
… | take 10
```

- Get few records - to familiarize yourself with the data. No actual order ensured.

```
… | where Timestamp > ago(1) and UserId = 'abdcdef'
```

- Filtering on a specific fields

```
… | project Col1, Col2, …
```

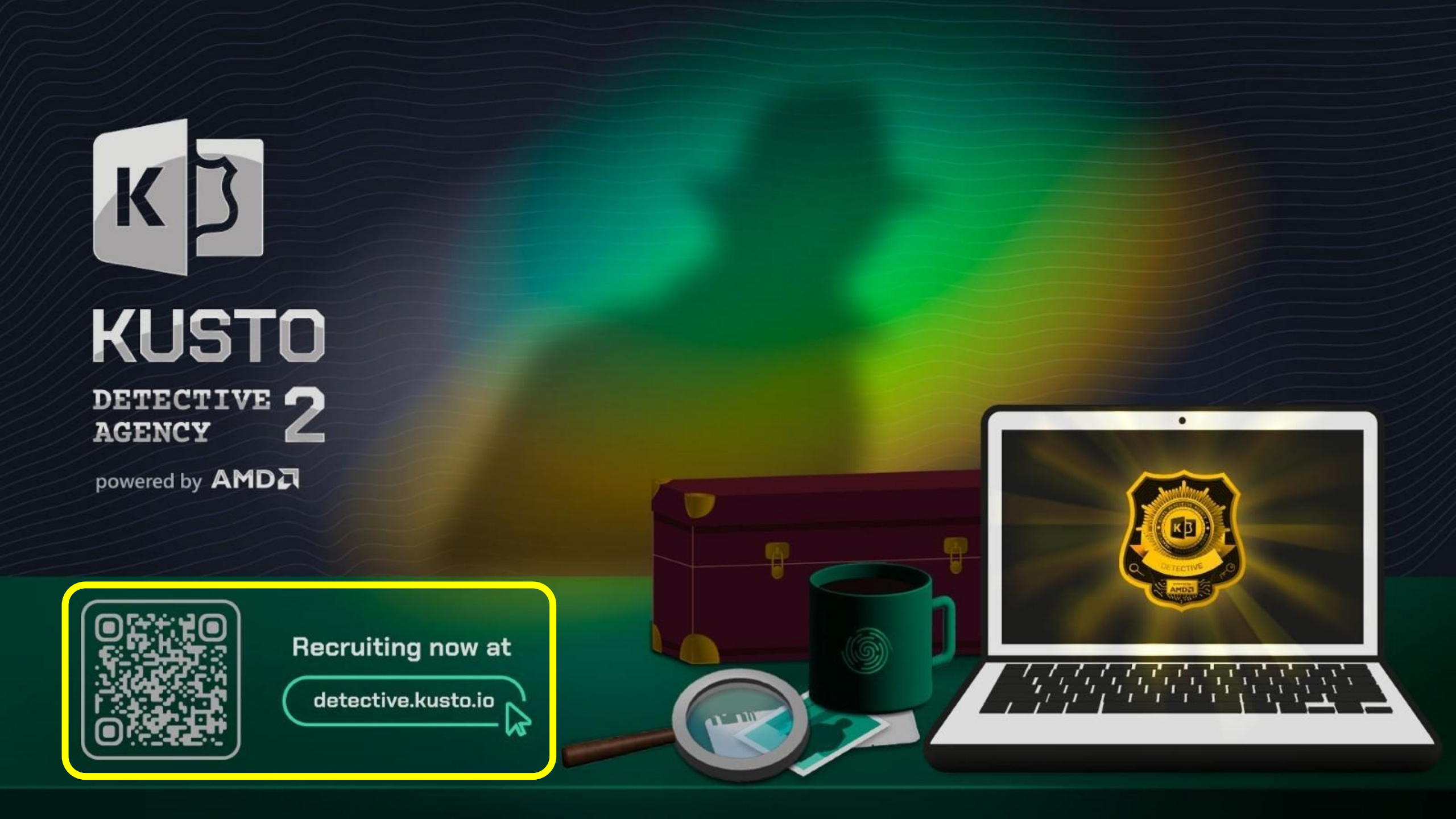
- Choose some columns (great if input table has dozens of columns)

```
…| extend NewCol1=Col1+Col2
```

- Introduces new calculated columns

```
… | render timechart
```

- Render data into a visual plot while exploring.


KUSTO
DETECTIVE AGENCY 2
powered by AMD
Recruiting now at
detective.kusto.io

Onboarding

1. Click Log-In if you've been here before.
2. Otherwise, create a free Kusto cluster at https://aka.ms/kustofree
3. You'll need either a Microsoft account (MSA) or an Azure Active Directory (AAD) identity.
4. Run the script, then attempt to solve the challenge.
5. Who is the detective that earned most money in 2022?

Onboarding – Tips & Hints

1. There are different detectives working on cases to get bounties
2. Only the first detective to crack the case gets the bounty
3. We are asked to find the detective that earned the most money in 2022
4. Extract the `Bounty` per case and filter on `EventType` for solved cases.
5. Leverage `let` statements, `arg_min()` & `sum()`.

Case 1: To bill or not to bill?

1. Bills are calculated for per house, based on water and electricity consumption.
2. Usage pattern has not changed, yet total bills have risen.
3. What is the total bills amount due in April?
4. Click the 💡 💡 💡 for hints
5. Click *Train me for the case*, it has valuable information.

Case 1: Tips & Hints

1. Look at the data in both tables.
2. Metric reporting is error prone & sometimes sent again.
3. Leverage distinct, lookup, extend and sum().

Case 2: Catch the Phishermen!

- A phishermen is making calls in attempt to steal identities.
- What phone number is used for placing the phishing calls?

2nd Case – Tips & Hints

1. We see some calls are Hidden.
2. It's common for Destination to disconnect when spammers call.
3. What is the most suspicious Origin that called the most Destination?
4. Leverage join (inner), dcount() & lessons this far.

Resources | Eval

- aka.ms/StartKqlVideo
- aka.ms/learn.kql
- aka.ms/adxinaday
- aka.ms/adx.pluralsight
- aka.ms/adx.try
- aka.ms/adx.youtube
- aka.ms/adx.blog
- aka.ms/adx.sof