

Not your parent's Splunk, an SDC journey

.conf19

splunk>

Not your parent's
Splunk, an SDC
journey
SCS

.conf19

splunk>



Kyle Champlin

Principal Product Manager | Splunk



Raanan Dagan

Principal SE Architect | Splunk

Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Demo

Live Re-enactment

Agenda

What is SCS, Splunk Investigate

Splunk Enterprise vs SCS

The journey of building our first app with SCS

- Use Case and Dataset details
- Highlight the fun parts and the foibles

SCS detail steps to create out first App

- Create indices via the Catalog Service
- Using Data Stream Processor for preparation and ingestion
- Investigate and analyze using Workbooks
- Build dashboards to share and present



What is SCS

Splunk Cloud Services Basics

Splunk Cloud Platform

SCS-Powered Applications

*Machine-data driven products that Splunk and partners take to market, for a range of buyers and personas.
(e.g. Splunk Investigate, Mission Control)*

Splunk Developer Cloud

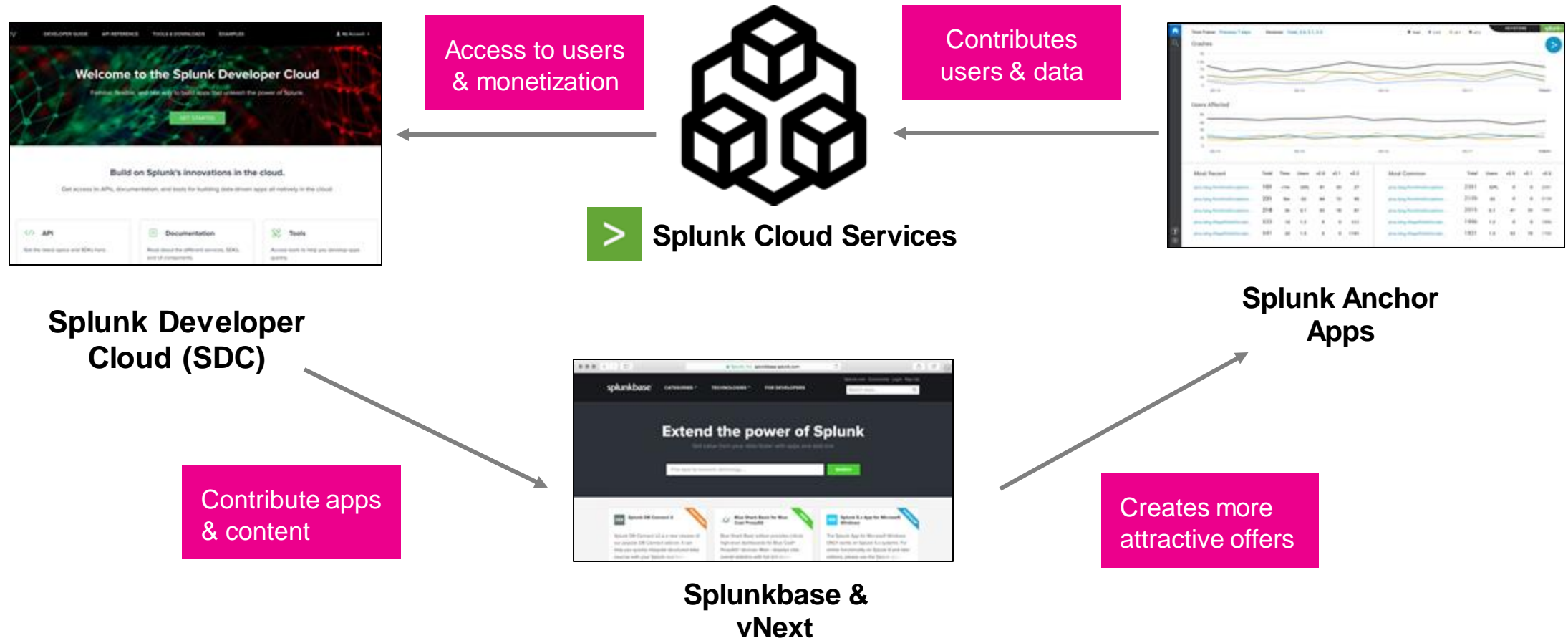
*Tooling, components, and guidance for modern application development.
(e.g. SDKs, CLI, Code examples)*

SCS Services and Modules

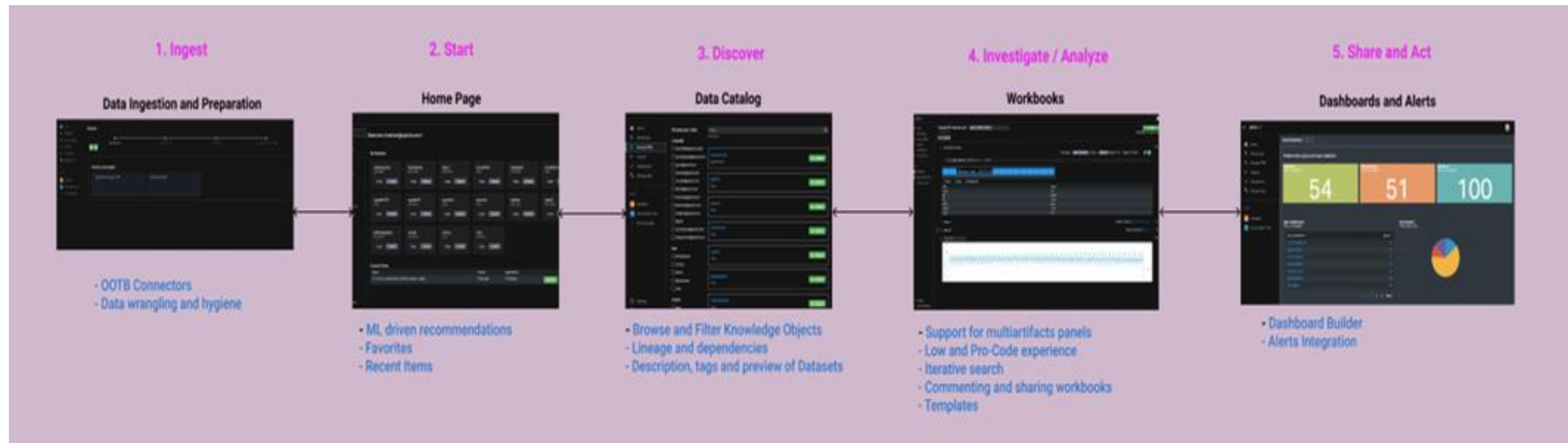
*The core modules and services required to build multi-tenant, scalable data-driven applications.
(e.g. Data Ingest, Search, Alerting)*

Splunk Cloud Services

SCS & SCS-Powered Apps



SCS Core Capabilities





Enterprise vs SCS

Splunk Core vs SCS Comparison

Wait...where's btool?

Splunk Core

- SimpleXML
- \$SPLUNK_HOME/bin/splunk help
- UF, HEC, File upload, etc.
- .conf system

SCS

- Dashboarding Framework
- scloud help OR
- Ingest Service & Streams Service
- Catalog Service



The journey of building our first app with SCS

The use case

Use Case and Dataset Details

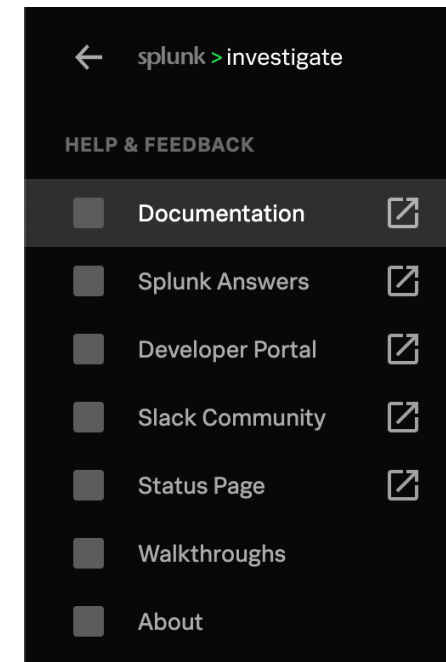
Will You Be Paying With Cash Or Card?

There are some long-standing things that are “complex” to do on Enterprise

- In particular, there is a use-case that Streaming tools demo well
 - Pull in some e-commerce Gaming data
 - Tag data as either credit-card or cash and process/treat that data separately
 - **Before** indexing the credit-card data, redact everything but the last 4 digits
 - Based on its payment type, send to a **separate index** (cash or cc)

Could we do this with SCS/Investigate in less than a day?

- Knowing nothing about the technical details of SCS
- Not having any prior exposure to the dataset



```
A5D125F5550BE7822FC6EE156E37733A,08DB3F9FCF01530D6F7E70EB88C3AE5B,Credit Card,14,2018-01-13 04:37:00,2018-01-13 04:47:00,-73.966843,40.756741,4539385381557252
1E65B7E2D1297CF3B2CA87888C05FE43,F9ABCCCC4483152C248634ADE2435CF0,Game Card,16.5,2018-01-13 04:26:00,2018-01-13 04:46:00,-73.956451,40.771442,
EE1513D432B07F7E0B5E2ED1EF629086,F31D261881520931062C011366E56A04,Credit Card,22.7,2018-01-13 04:30:00,2018-01-13 04:44:00,-74.005455,40.740772,348850543617913
90D83E0D0B4FF8DE2923C2977EF22C36,92153937578731DA2B1EC83D91E7FA3E,Game Card,9.5,2018-01-13 04:37:00,2018-01-13 04:44:00,-73.998657,40.74015,
```

↑
Amount Spent per game

↑
Credit Card in the Clear

DSP For Fun & Profit


Services, Documentation & Hella Parenthesis

Having no prior exposure to DSP we were both shocked & amazed

- Incredibly feature rich – the docs were very dense
- Solid UI experience – you can create, edit and preview your work, no /debug/refresh required
- The DSL has a pretty steep learning curve, but is powerful
 - We ended up with a lot of this sort of thing

Once the data started flowing into our indices

- The dashboarding experience was refreshing
- There are some workflow differences
 - “Sharing” things isn’t like it used to be



```
1  as(if(match-regex(cast(get("Credit_Card"),"string"),/^4.*/),"Visa",
2  if(match-regex(cast(get("Credit_Card"),"string"),/^5[1-4].*/),"MasterCard",
3  if(match-regex(cast(get("Credit_Card"),"string"),/^3[4,7].*/),"AMEX",
4  if(match-regex(cast(get("Credit_Card"),"string"),/^30[0-5]13[6,8].*/),"Diners Club",
5  if(match-regex(cast(get("Credit_Card"),"string"),/^6011|65.*/),"Discover",
6  if(match-regex(cast(get("Credit_Card"),"string"),/^2131|1800|35.*/),"JCB","Unknown"))))))
7  ,"Card_Type");
8  |
```



SCS detailed steps to create out first App

An “App” in 2 Hours


Create indices and data catalog

Credit Card and Cash Indexes

What is this Data Catalog/Catalog Service?

- “*With the Metadata Catalog you can create and manage knowledge objects such as datasets, fields, rules, actions, dashboards, and workflows.*”

Effectively it allows us to define various configurations

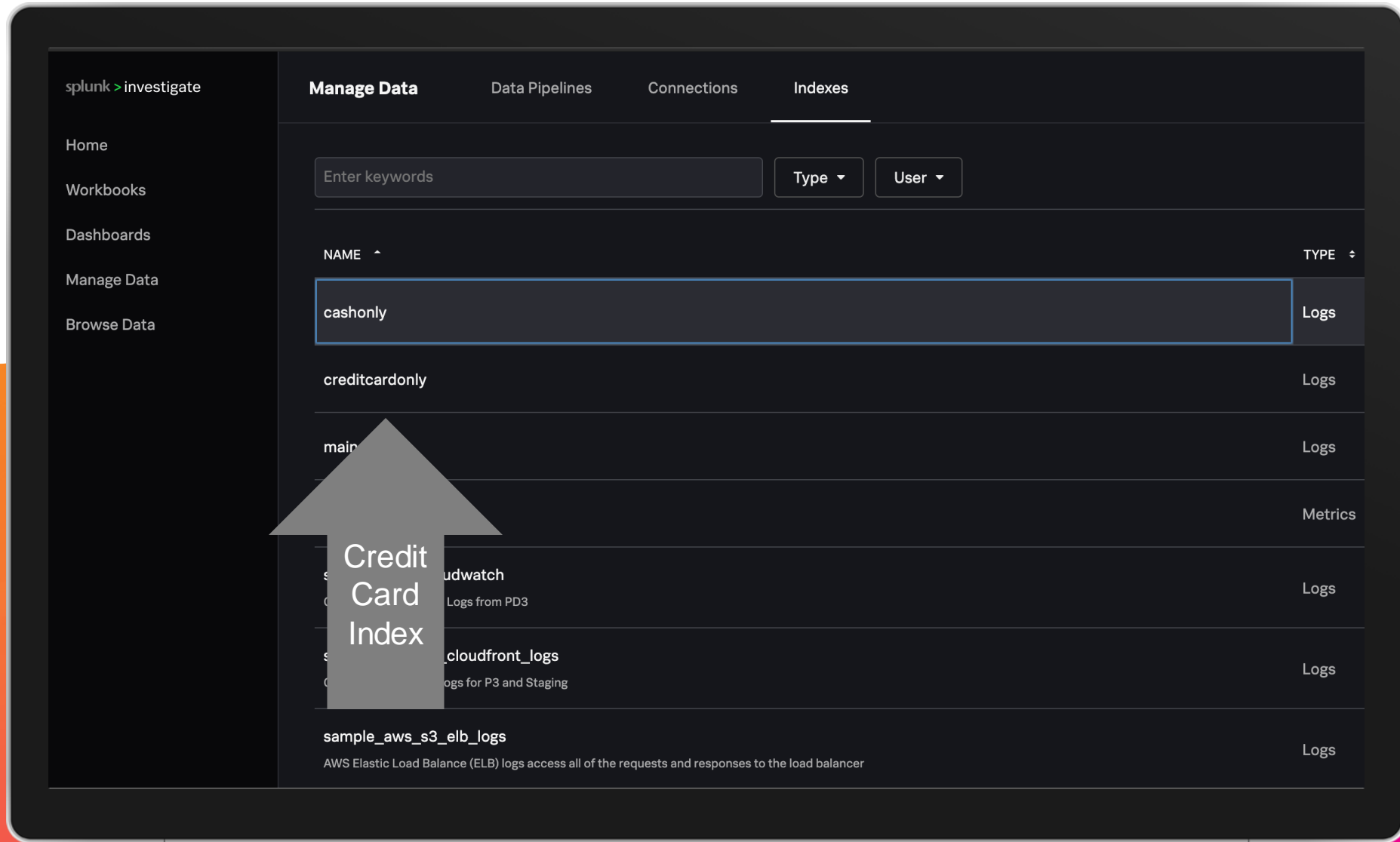
- We used scloud to do this 
- But you can use dev portal!
- Now we have new indices to sink to in DSP!

```
(kchamplin) >>> scloud catalog help
```

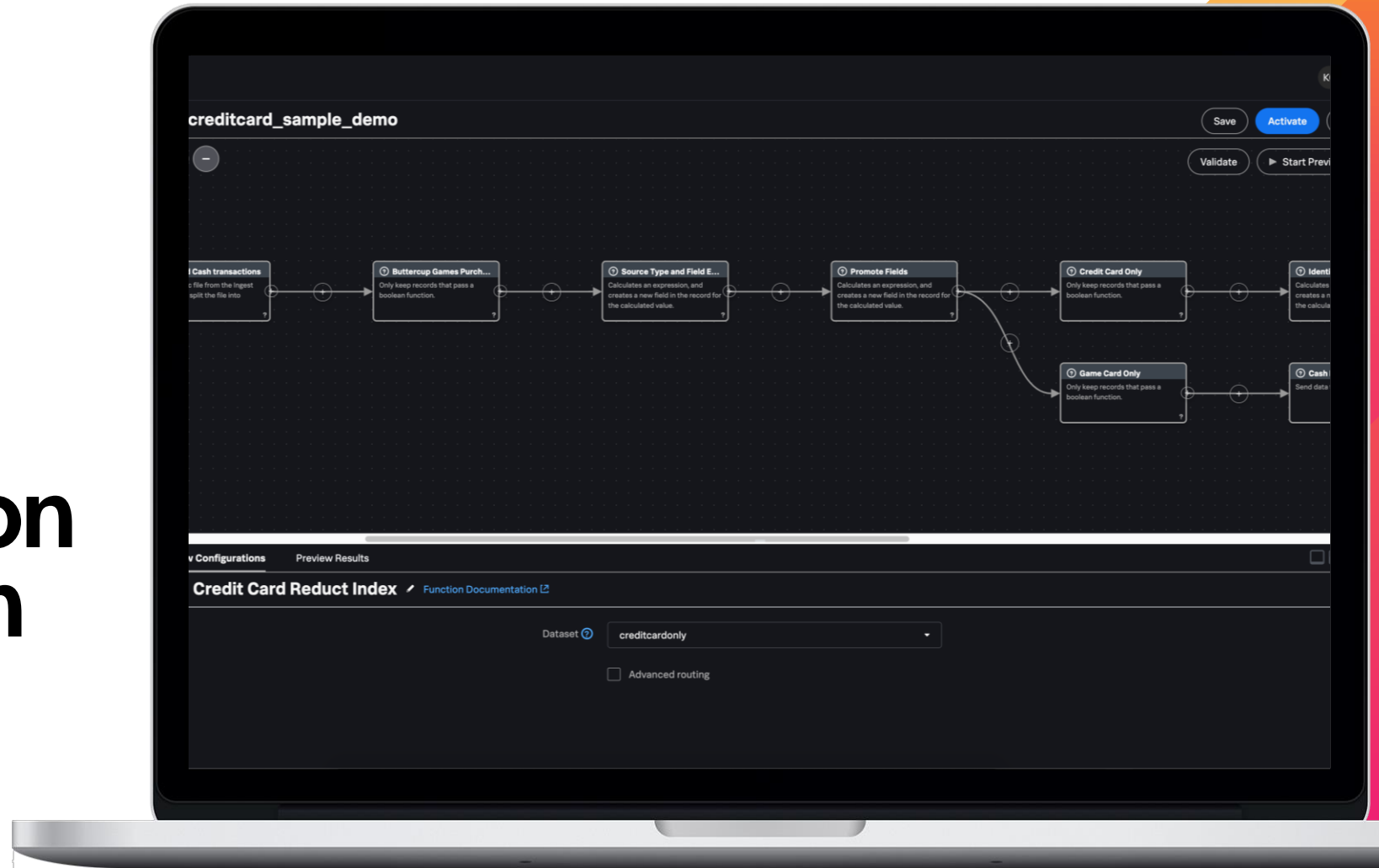
```
create-dataset <dataset-name>
lookup|kvcollection||metric|index [-owner <user-id>]
  [-module <module-name>] [-read-roles <role-name>] [-
write-roles <role-name>]
  [-case-sensitive-match true|false] [-external-kind
<lookup-type>]
  [-external-name <lookup-name>] [-filter true|false] [-
max-matches true|false]
  [-min-matches true|false] [-default-match true|false] [-
disabled true|false]
  [-fields true|false]
```

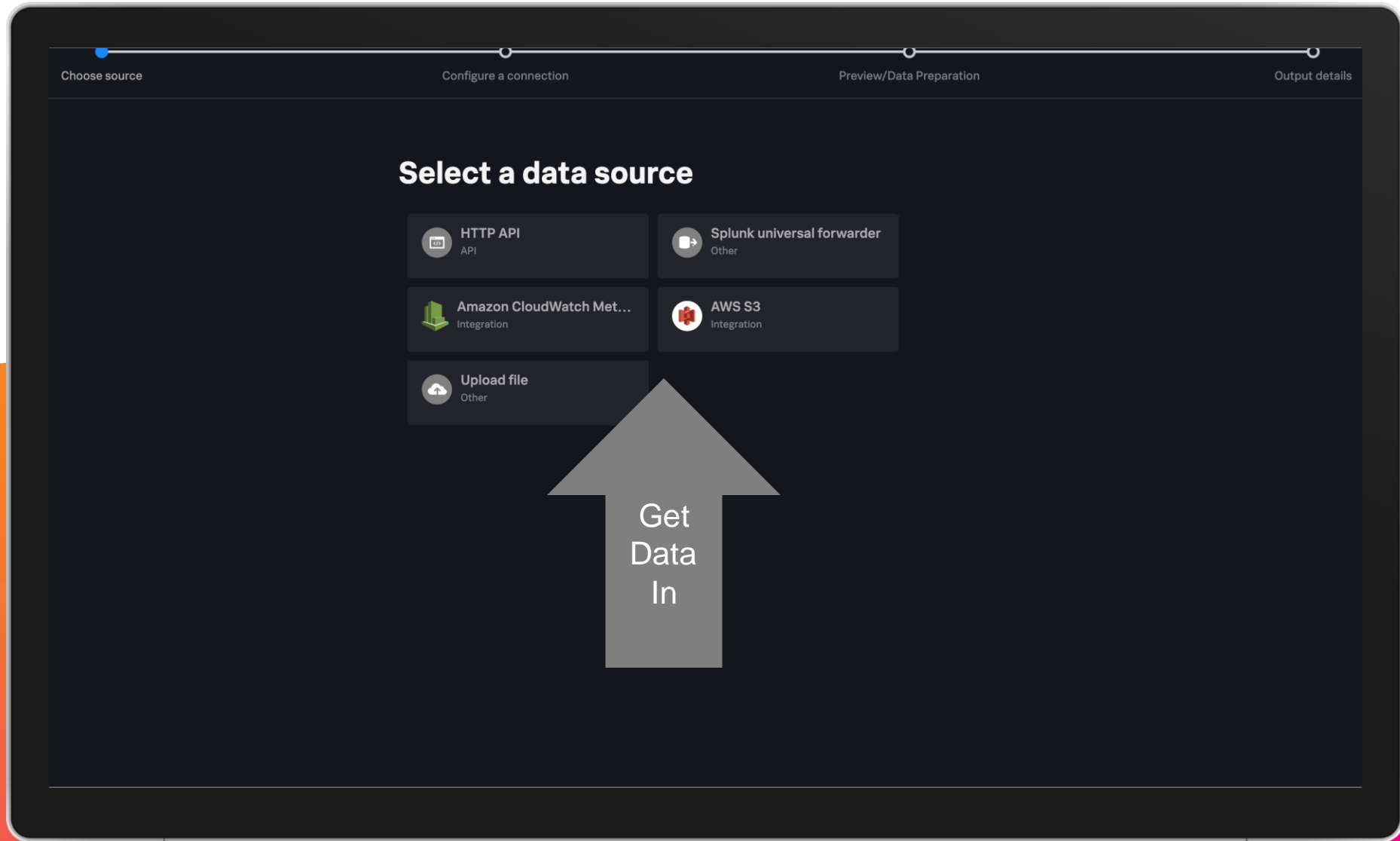
Create an index dataset:

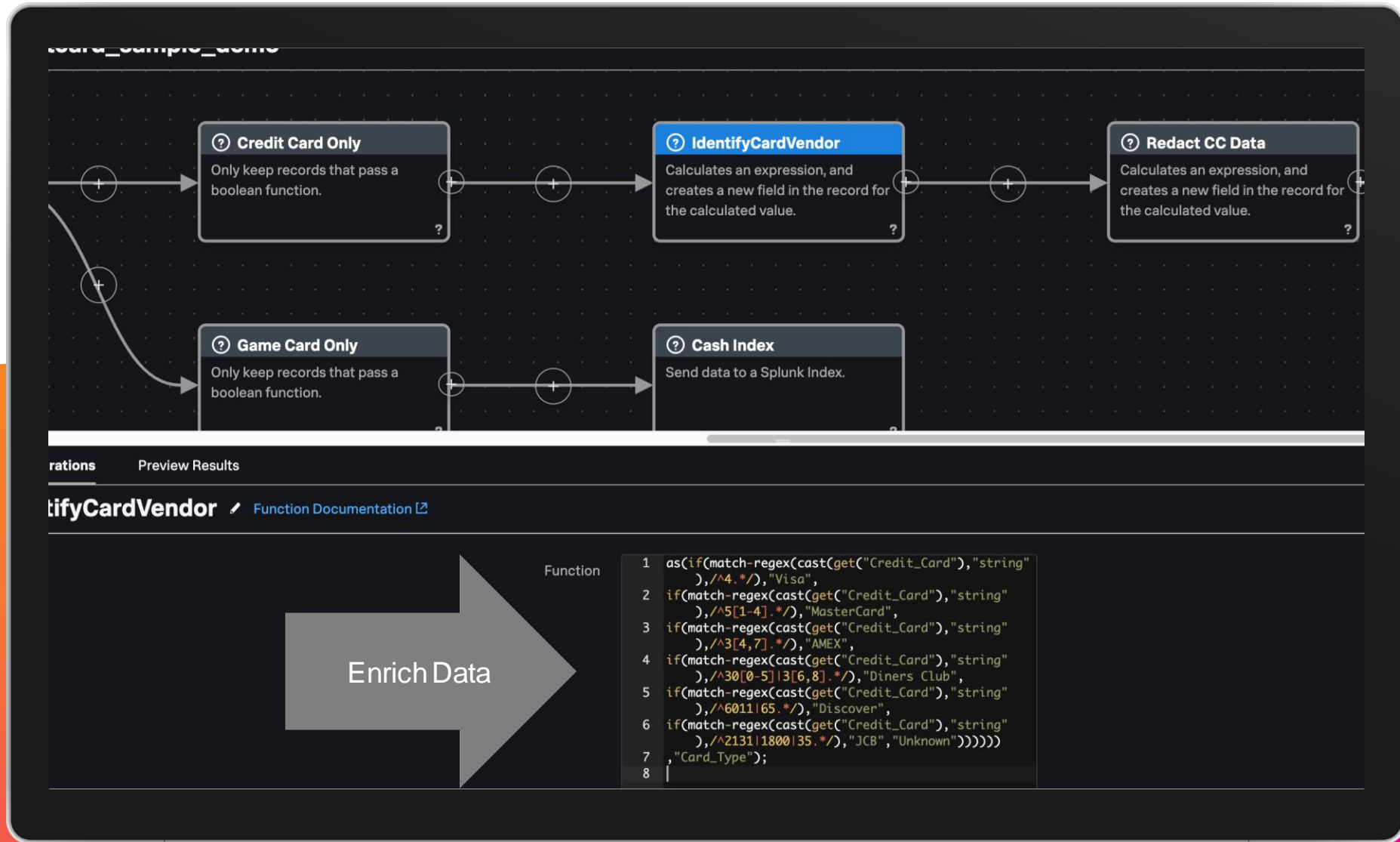
```
$ scloud catalog create-dataset index credit_card
disabled=false
```



Using DSP (part of SCS) for preparation and ingestion

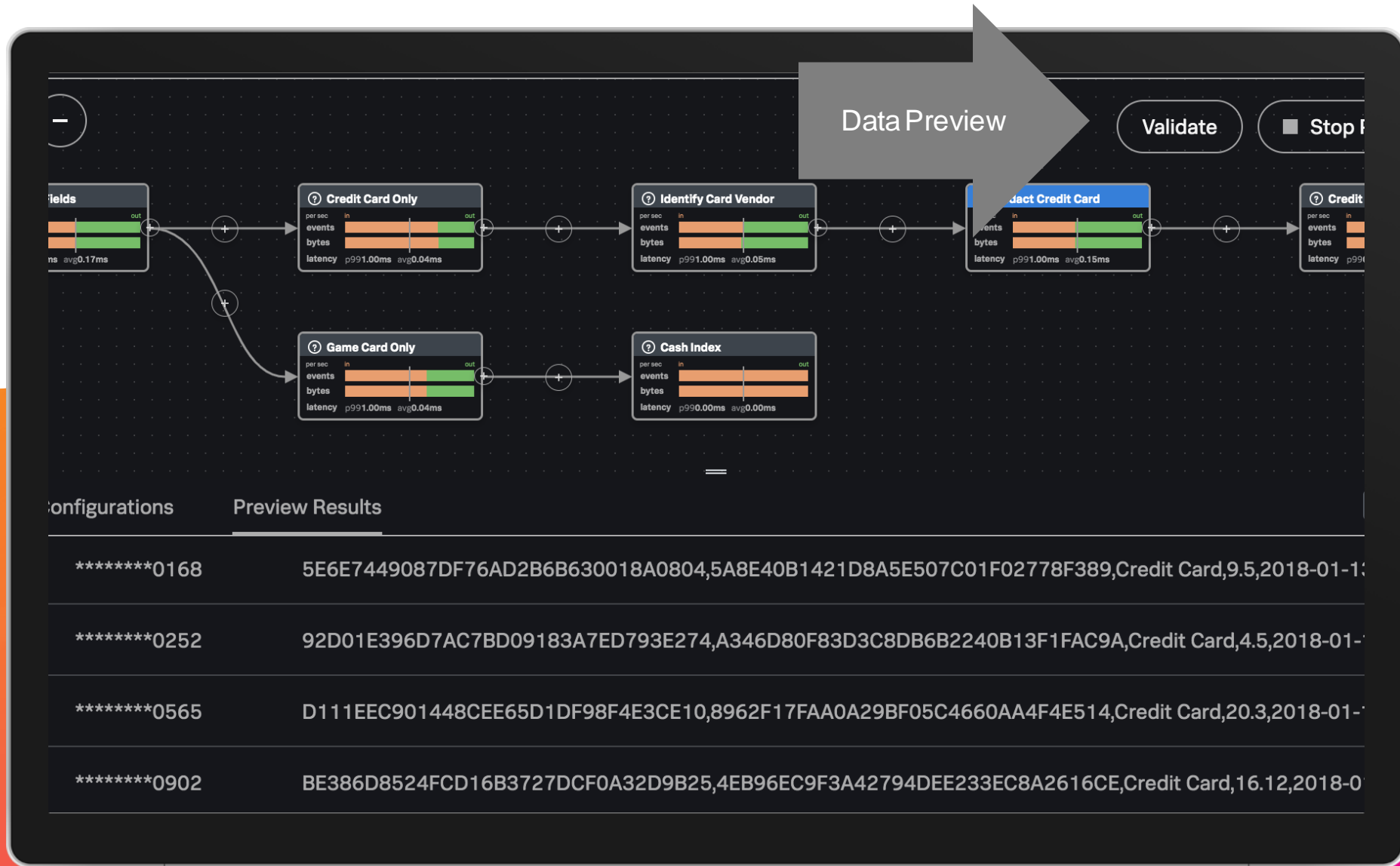




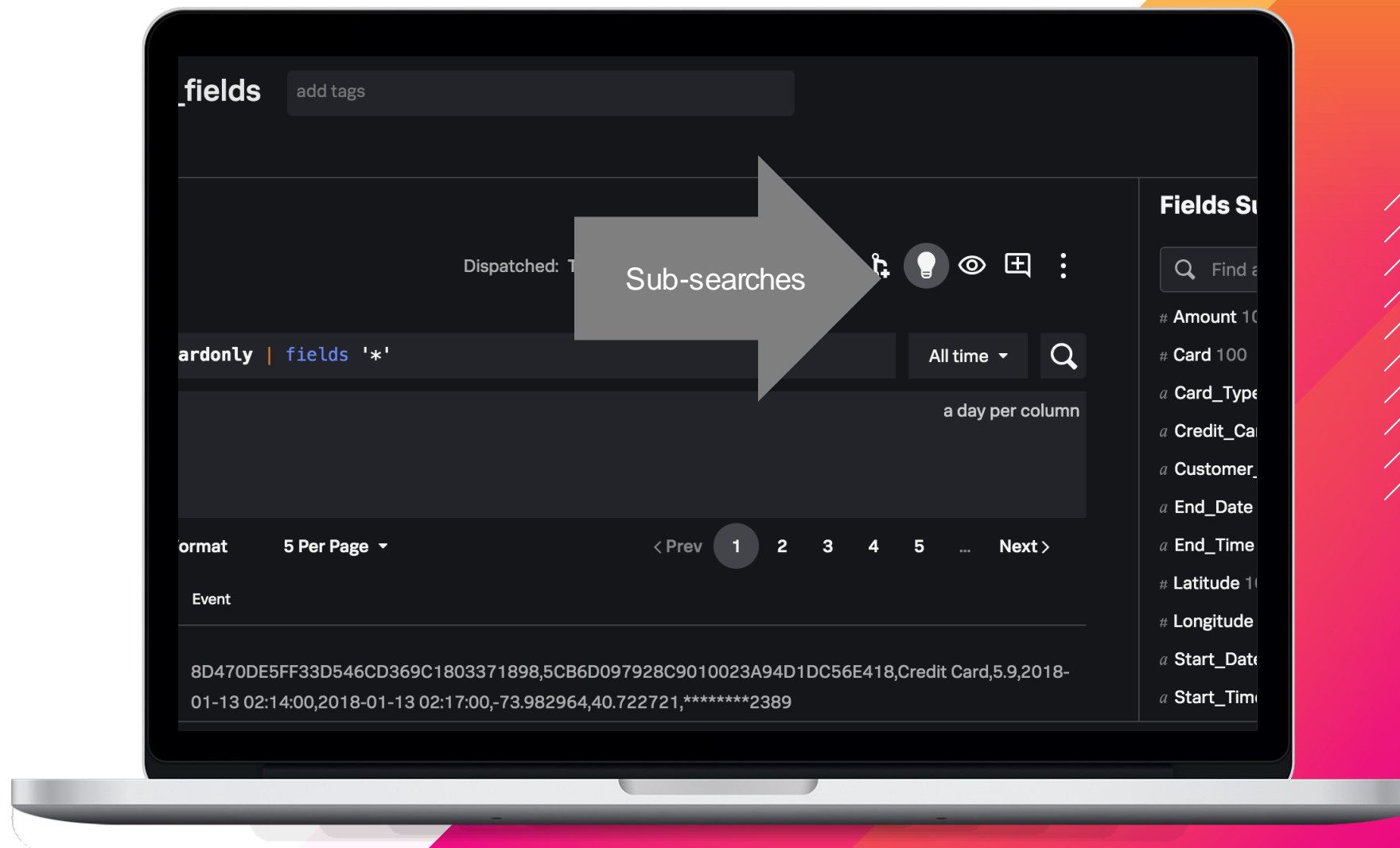


The screenshot displays the Splunk Search Processing Language (SPL) interface. At the top, a search bar contains the query `Mask CC`. Below the search bar, the 'Functions' section is visible, with the 'Redact CC Data' function selected. The function's description states: 'Calculates an expression, and creates a new field in the record for the calculated value.' Below this, the 'Function Documentation' link is shown. The 'Function' section displays the following code:

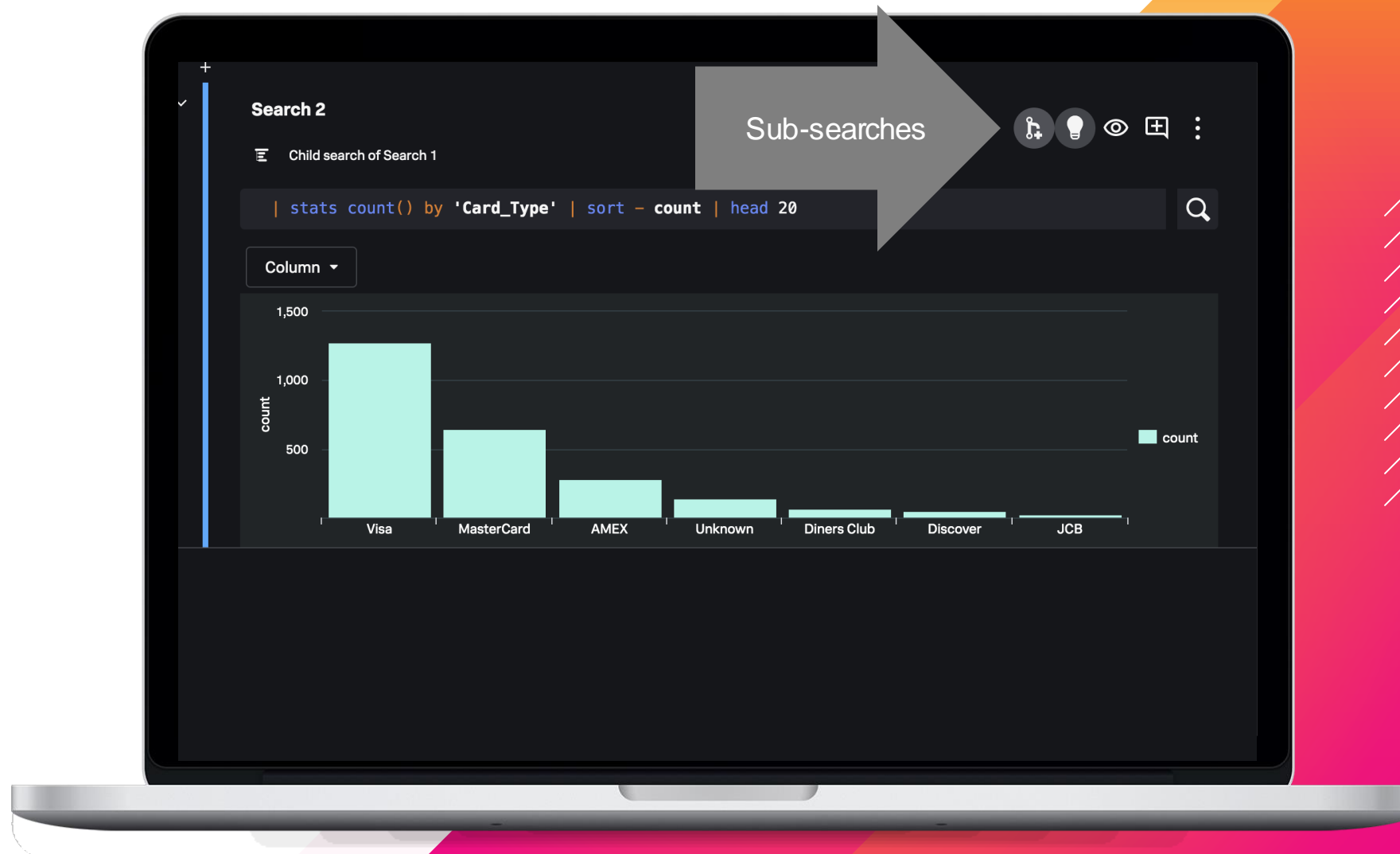
```
1 as(replace(cast(get("Credit_Card"),"string"),/[1-5][0-9]{11}([0-9]{4})/, "*****$1"),  
  "Credit_Card");  
2 as(replace(cast(get("body"),"string"),/[1-5][0-9]{11}([0-9]{4})/, "*****$1"), "body");  
3
```



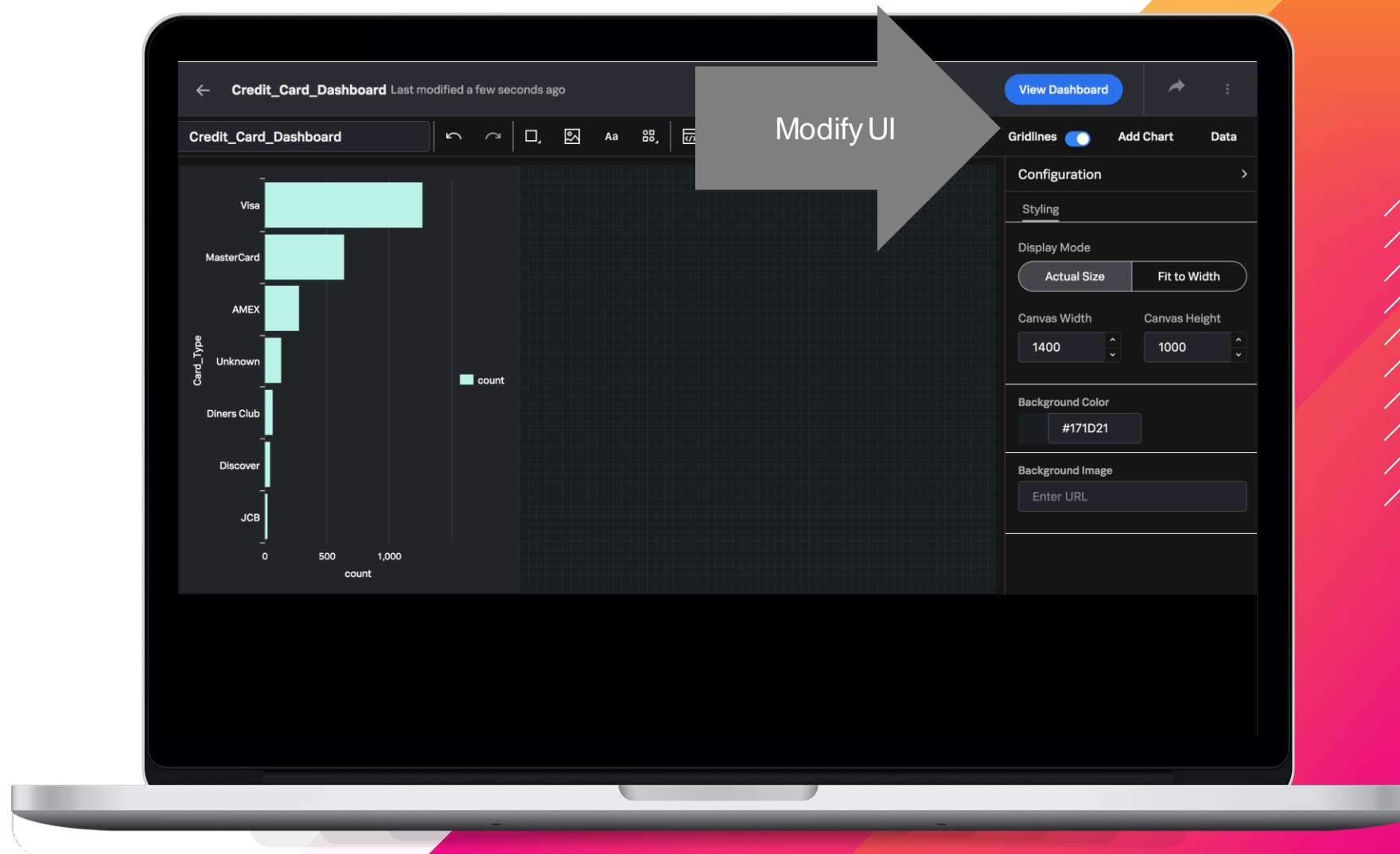
Using Workbooks for Creating Searches



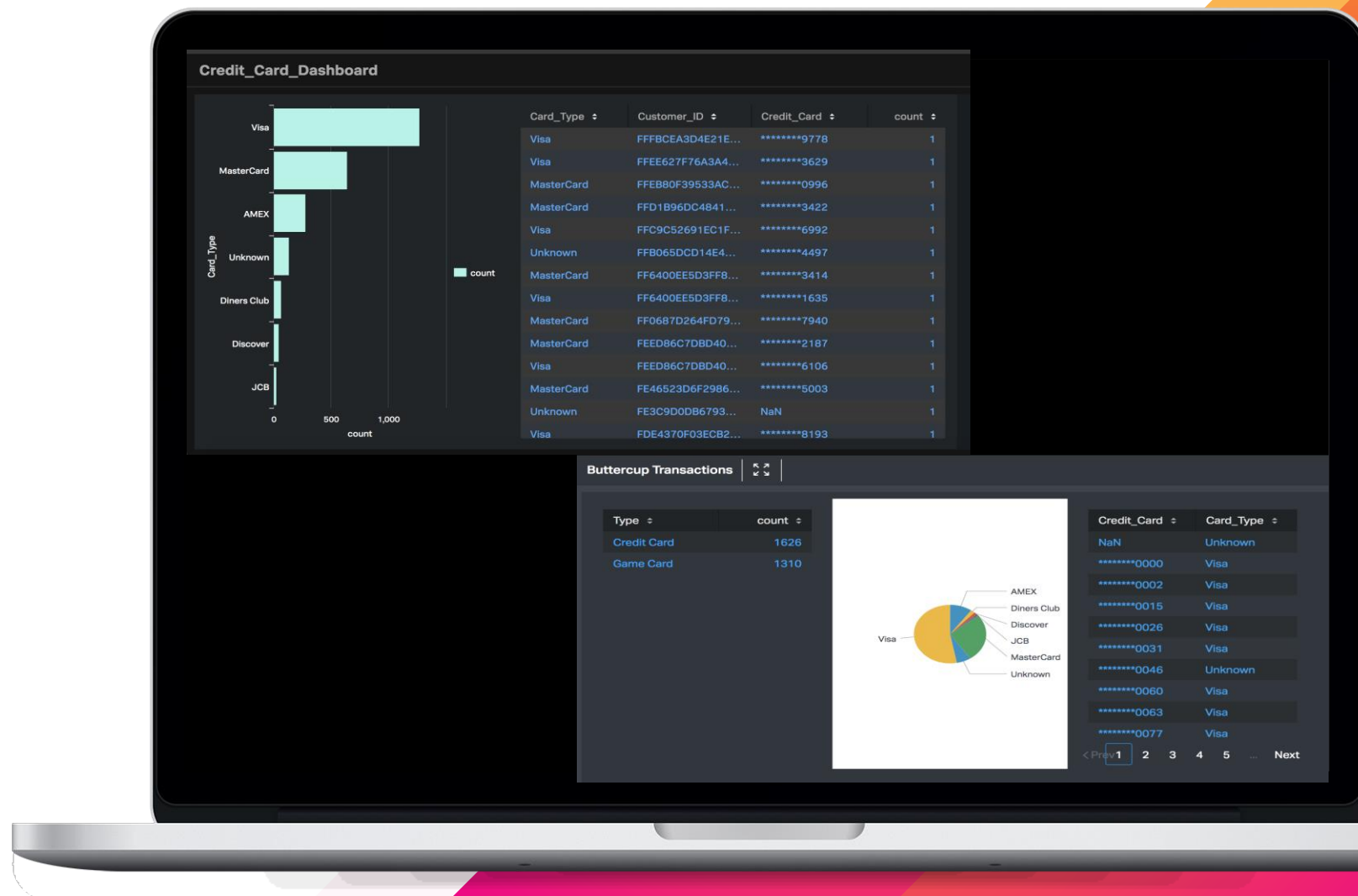
Using Workbooks for Creating Searches



Using Dashboards for Sharing



Using Dashboards for Visualization





Q&A

Kyle Champlin | Senior Product Manager
Raanan Dagan | Principal SE Architect

Key Takeaways

1. You can teach an old Pony new tricks
2. An App in 2 Hours
3. No Infrastructure is cool



Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION

