Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

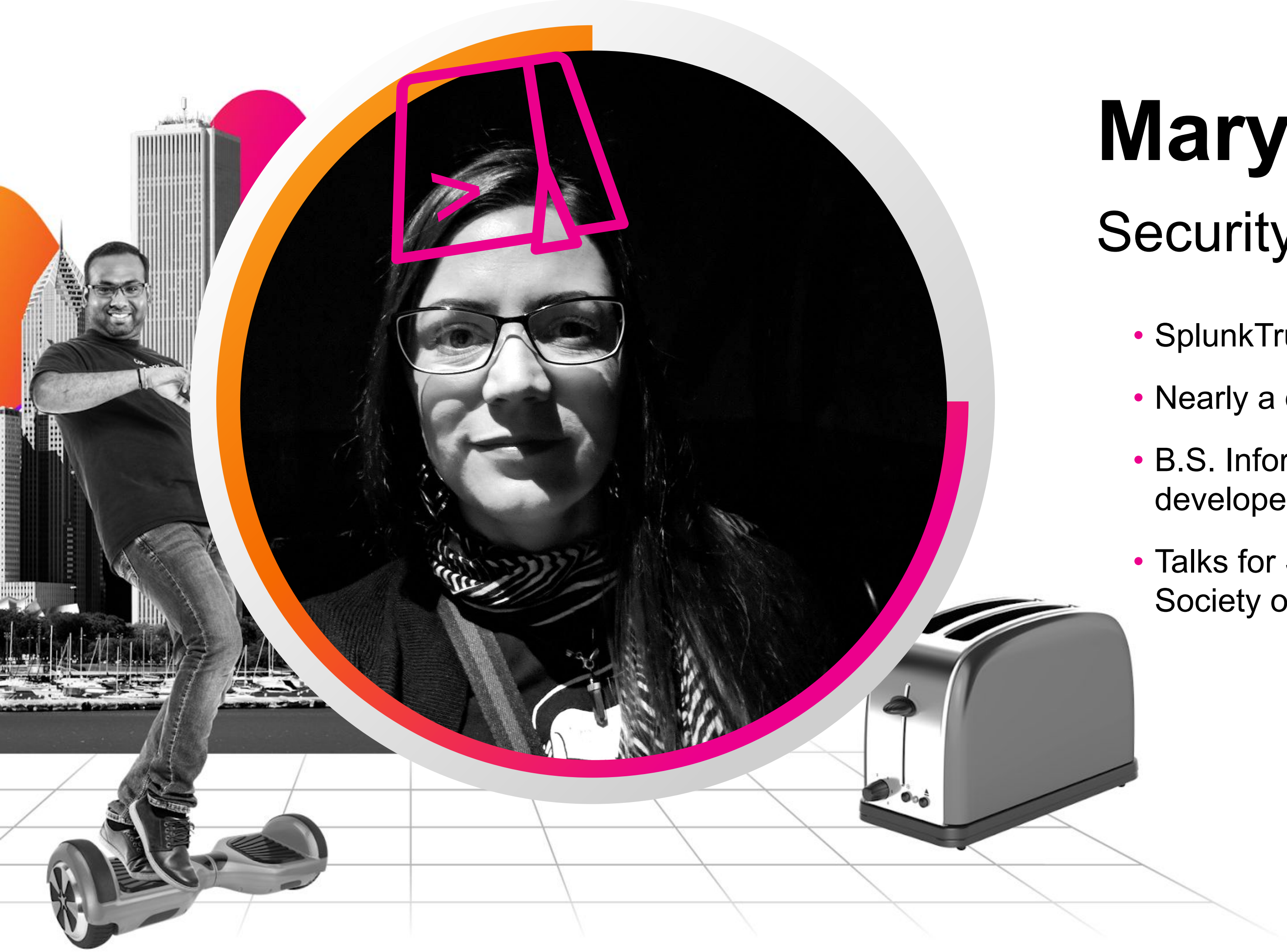
For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Dynamic Splunk Data Delivered Where Your Executives Live

PLA1122B

Mary Cordova
Security Operations



Mary Cordova

Security Operations

- SplunkTrust member & Splunk® Certified Architect
- Nearly a decade in SOC, SIEM, SOAR, IR, & Data Analytics
- B.S. Information Systems, 6xSANS, CCNA, SSCP, ISC^2 exam developer, CompTIA A+
- Talks for Splunk .conf® & User Groups, Shellcon, Women's Society of Cyberjutsu, San Diego DFIR Meetup

splunk> .conf22

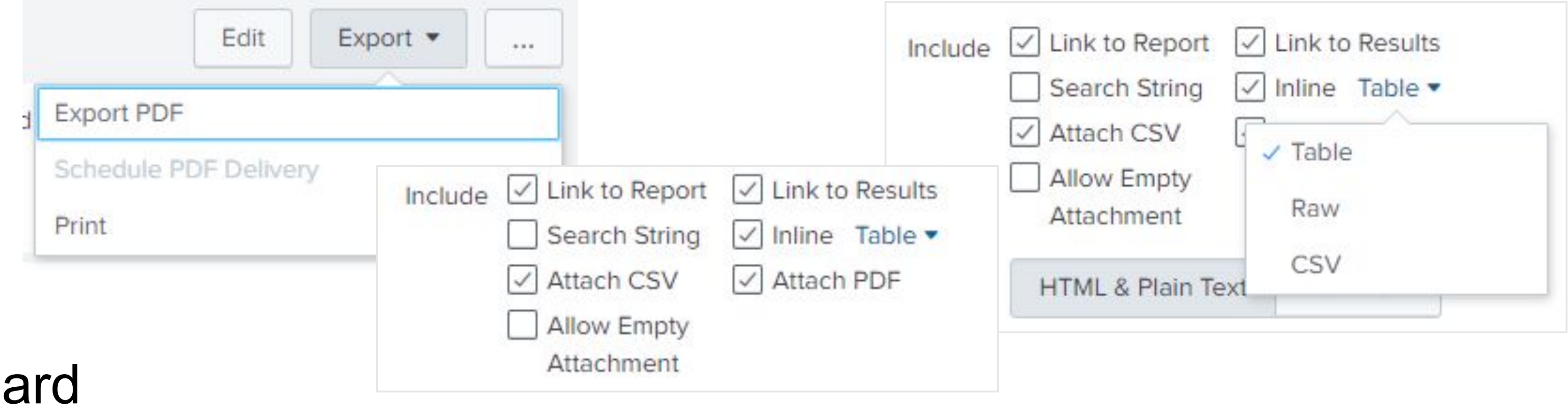
Why Not Use Splunk for Everything?

How I learned to kinda love PowerBI®

- **Access**
- **Skills**
- **Audience**
- **Platform/Format**

- Not everybody had access to Splunk
- There was a learning curve
- They might need to share the content with someone else who didn’t have access or skills
- They just wanted a slide deck
- **And the email, export, & iframe options in Splunk are ☹**

What Options* Did I Look Into?



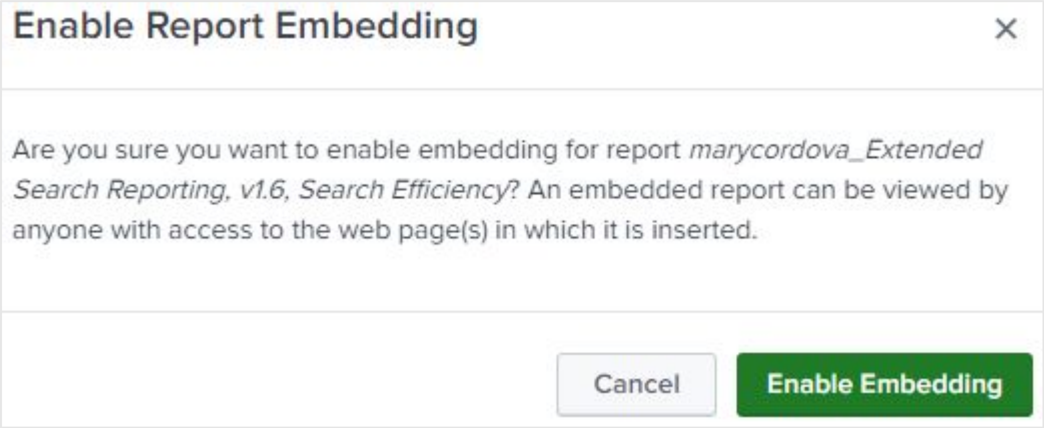
Include
☑ Link to Report ☑ Link to Results
☐ Search String ☑ Inline Table ▾
☑ Attach CSV ☑ Attach PDF
☐ Allow Empty Attachment

Include
☑ Link to Report ☑ Link to Results
☐ Search String ☑ Inline Table ▾
☑ Attach CSV
☐ Allow Empty Attachment

✓ Table
Raw
CSV

HTML & Plain Text

- Export & email dashboard
- Export & email reports
- Embed reports iframes

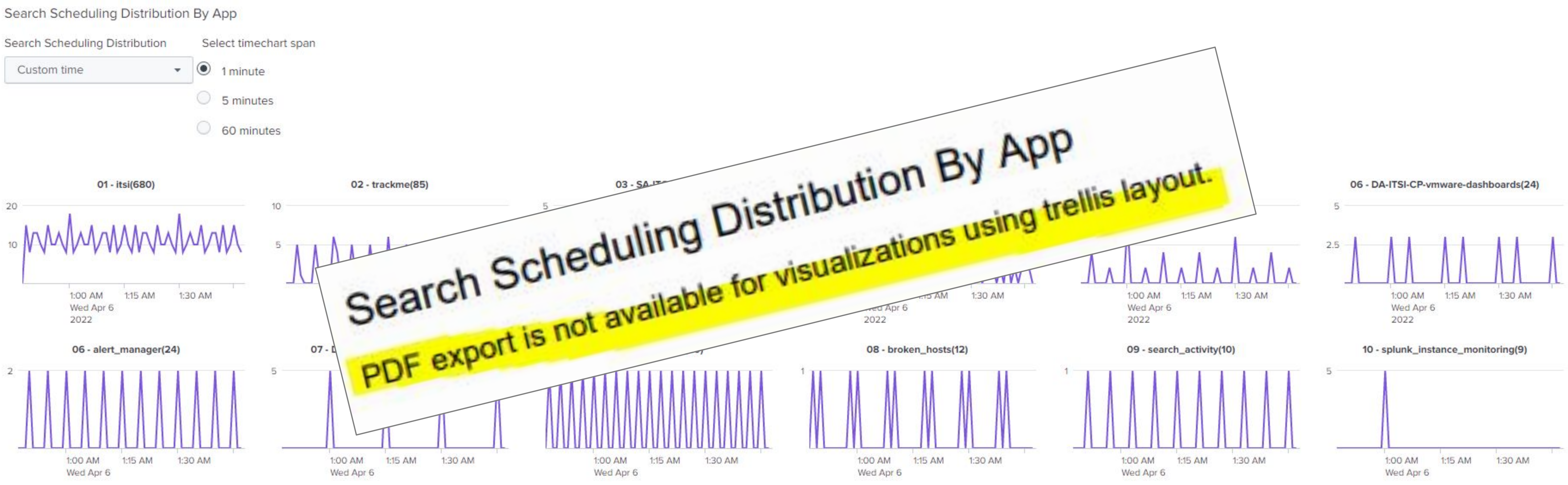


Enable Report Embedding

Are you sure you want to enable embedding for report *marycordova_Extended Search Reporting, v1.6, Search Efficiency*? An embedded report can be viewed by anyone with access to the web page(s) in which it is inserted.

*There's probably other options I don't know about and don't know how to use, but next year you can do that talk.

Dashboard Export



Search Scheduling Distribution By App

Search Scheduling Distribution: Custom time

Select timechart span

● 1 minute

○ 5 minutes

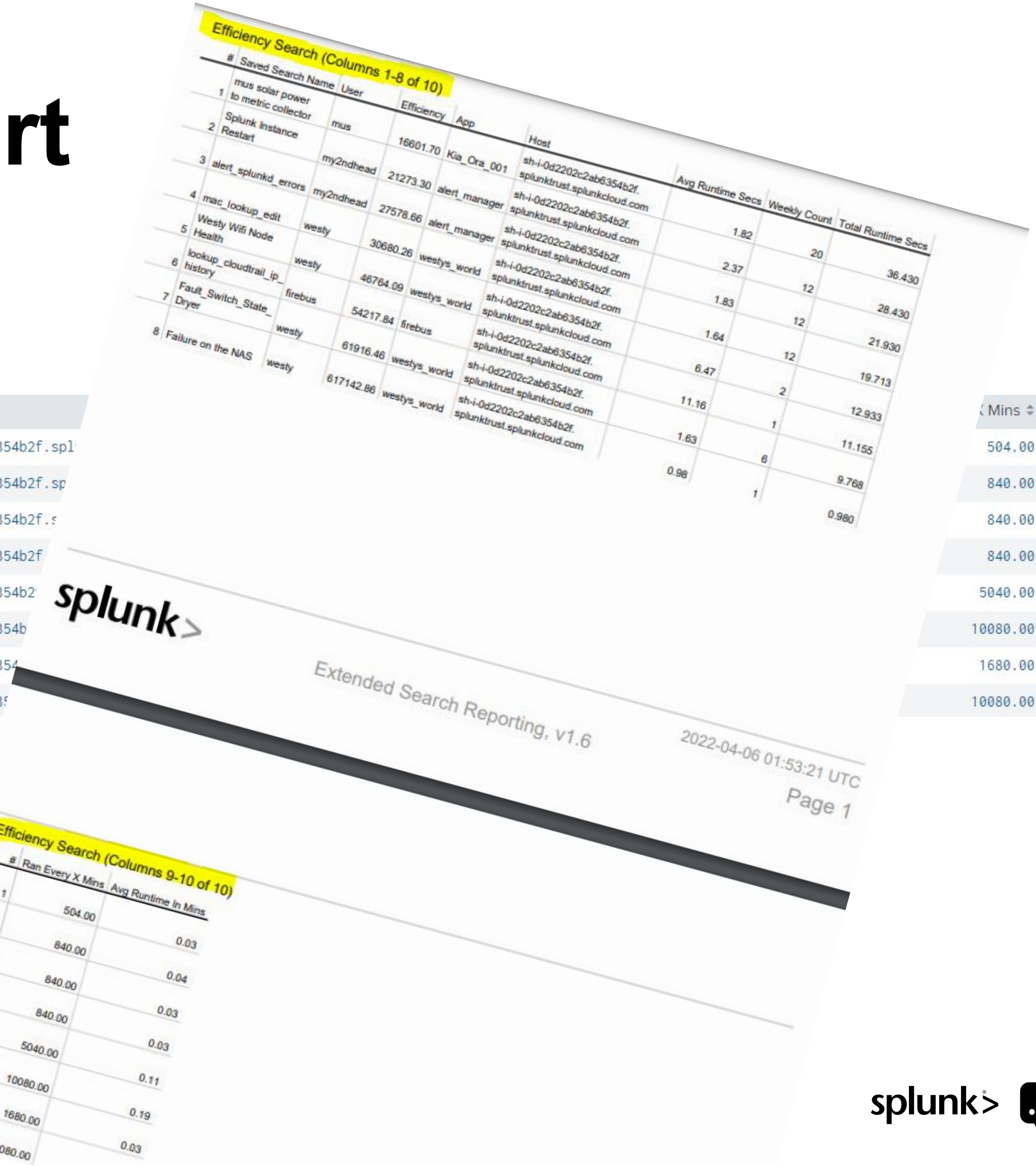
○ 60 minutes

Search Scheduling Distribution By App

PDF export is not available for visualizations using trellis layout.

Dashboard Export

Saved Search Name	User	Efficiency	App	Host	Mins	Avg Runtime In Mins
mus solar power to metric collector	mus	16601.70	Kia_Ora_001	sh-i-0d2202c2ab6354b2f.spl	504.00	0.03
Splunk Instance Restart	my2ndhead	21273.30	alert_manager	sh-i-0d2202c2ab6354b2f.sp	840.00	0.04
alert_splunkd_errors	my2ndhead	27578.66	alert_manager	sh-i-0d2202c2ab6354b2f.s	840.00	0.03
mac_lookup_edit	westy	30680.26	westys_world	sh-i-0d2202c2ab6354b2f	840.00	0.03
Westy Wifi Node Health	westy	46764.09	westys_world	sh-i-0d2202c2ab6354b2	5040.00	0.11
lookup_cloudtrail_ip_history	firebus	54217.84	firebus	sh-i-0d2202c2ab6354b	10080.00	0.19
Fault_Switch_State_Dryer	westy	61916.46	westys_world	sh-i-0d2202c2ab6354	1680.00	0.03
Failure on the NAS	westy	617142.86	westys_world	sh-i-0d2202c2ab63	10080.00	0.02



Efficiency Search (Columns 1-8 of 10)

#	Saved Search Name	User	Efficiency	App	Host	Avg Runtime Secs	Weekly Count	Total Runtime Secs
1	mus solar power to metric collector	mus	16601.70	Kia_Ora_001	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.82	20	36.430
2	Splunk Instance Restart	my2ndhead	21273.30	alert_manager	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	2.37	12	28.430
3	alert_splunkd_errors	my2ndhead	27578.66	alert_manager	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.83	12	21.930
4	mac_lookup_edit	westy	30680.26	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.64	12	19.713
5	Westy Wifi Node Health	westy	46764.09	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	6.47	2	12.933
6	lookup_cloudtrail_ip_history	firebus	54217.84	firebus	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	11.16	1	11.155
7	Fault_Switch_State_Dryer	westy	61916.46	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.63	6	9.768
8	Failure on the NAS	westy	617142.86	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	0.98	1	0.980

splunk>

Extended Search Reporting, v1.6

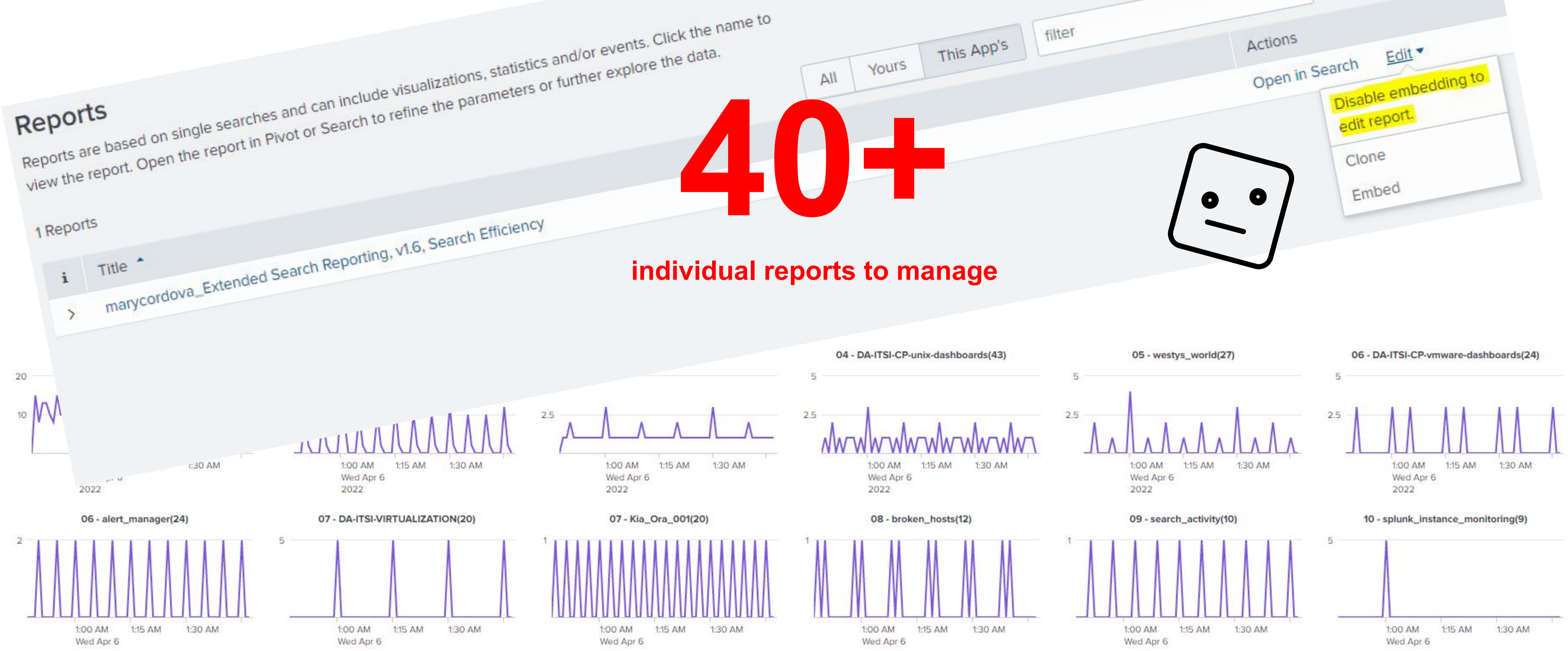
2022-04-06 01:53:21 UTC

Page 1

Efficiency Search (Columns 9-10 of 10)

#	Ran Every X Mins	Avg Runtime In Mins
1	504.00	0.03
2	840.00	0.04
3	840.00	0.03
4	840.00	0.03
5	5040.00	0.11
6	10080.00	0.19
7	1680.00	0.03
8	10080.00	

iframe Embedding



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

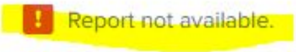
1 Reports

i	Title ▴	Actions
>	marycordova_Extended Search Reporting, v1.6, Search Efficiency	Open in Search Edit ▾

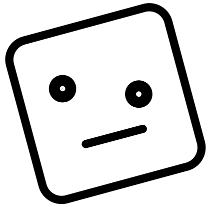
40+

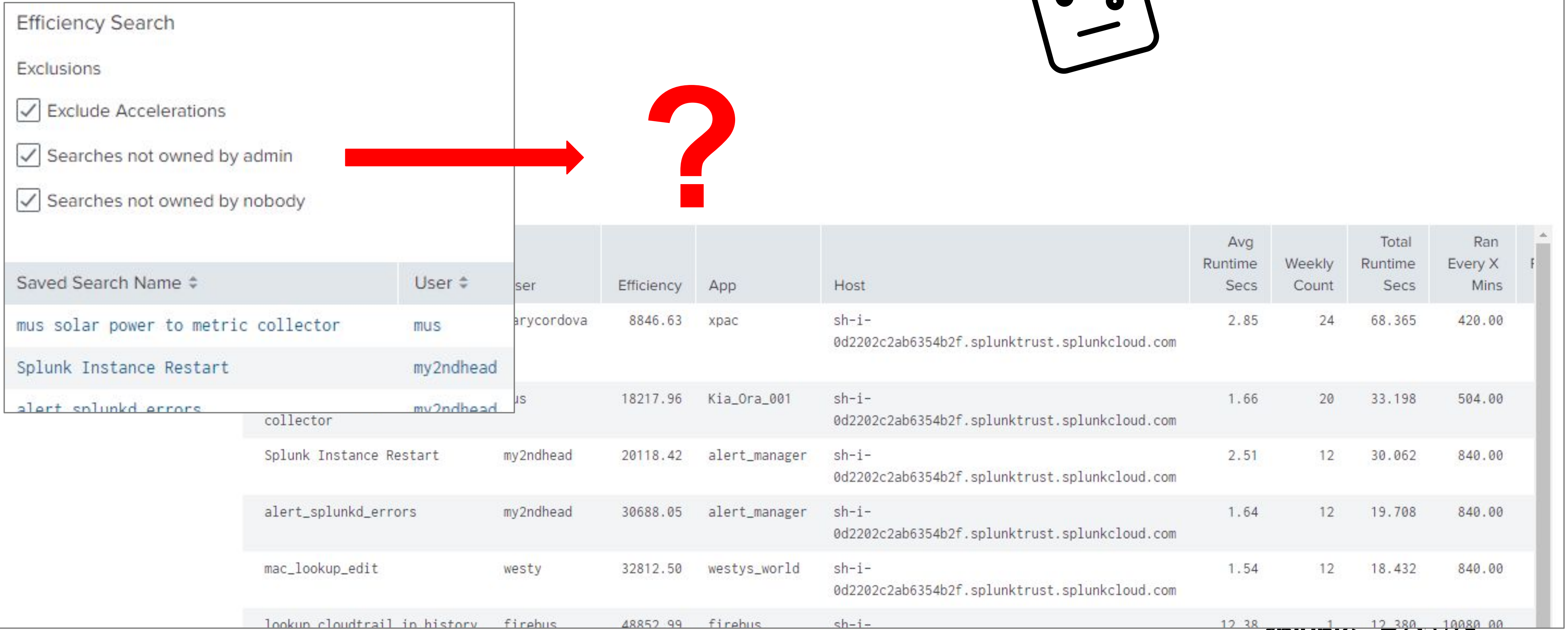
individual reports to manage

iframe Embedding



Report not available.





Efficiency Search

Exclusions

☑ Exclude Accelerations

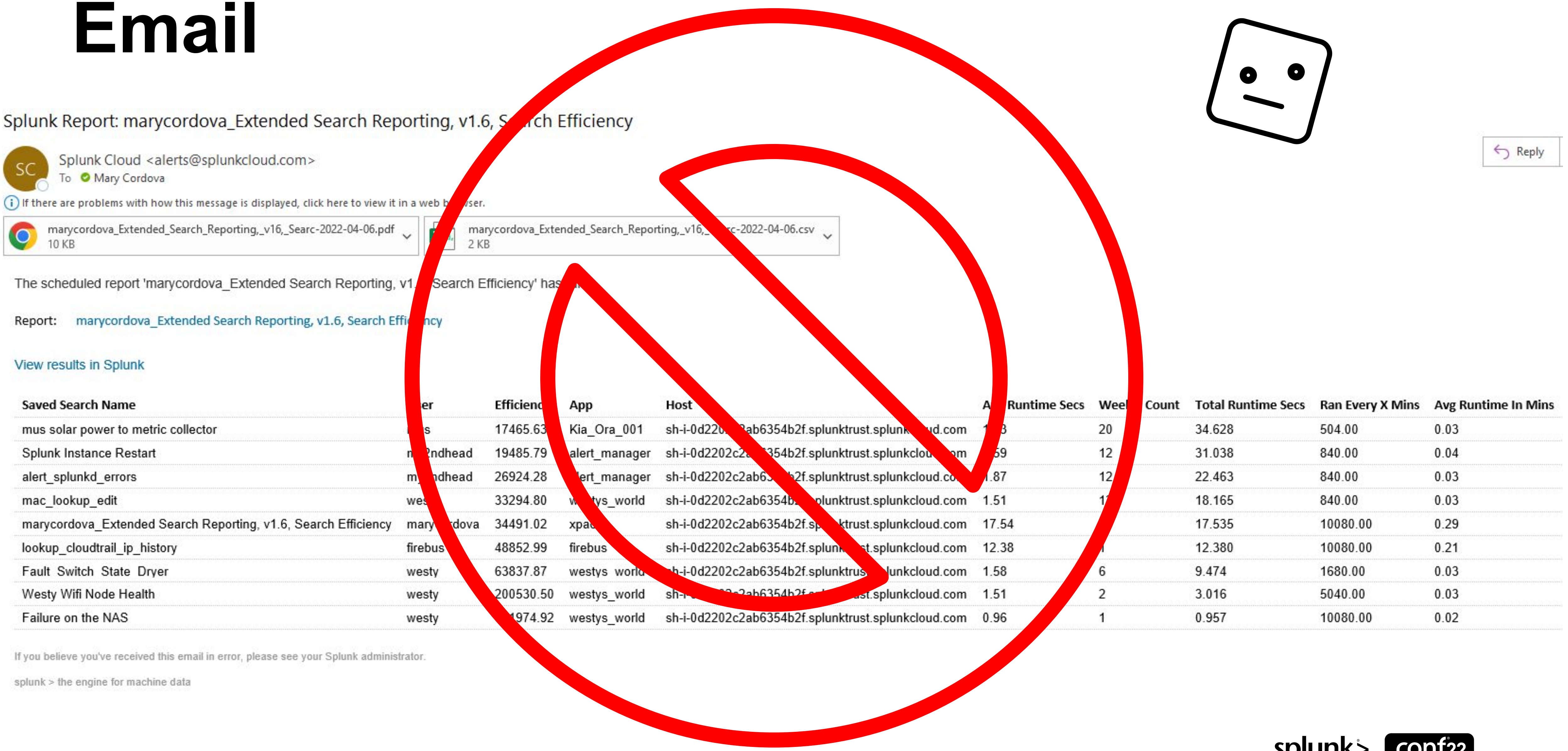
☑ Searches not owned by admin

☑ Searches not owned by nobody

Saved Search Name ⇕	User ⇕
mus solar power to metric collector	mus
Splunk Instance Restart	my2ndhead
alert_splunkd_errors	my2ndhead

	ser	Efficiency	App	Host	Avg Runtime Secs	Weekly Count	Total Runtime Secs	Ran Every X Mins
	rycordova	8846.63	xpac	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	2.85	24	68.365	420.00
collector	us	18217.96	Kia_Ora_001	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.66	20	33.198	504.00
Splunk Instance Restart	my2ndhead	20118.42	alert_manager	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	2.51	12	30.062	840.00
alert_splunkd_errors	my2ndhead	30688.05	alert_manager	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.64	12	19.708	840.00
mac_lookup_edit	westy	32812.50	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.54	12	18.432	840.00
lookup_cloudtrail_in_history	firebus	48852.99	firebus	sh-i-	12.38	1	12.380	10080.00

Email



Splunk Report: marycordova_Extended Search Reporting, v1.6, S rch Efficiency

Splunk Cloud <alerts@splunkcloud.com>

To Mary Cordova

If there are problems with how this message is displayed, click here to view it in a web b ser.

marycordova_Extended_Search_Reporting,_v16,_Searc-2022-04-06.pdf
10 KB

marycordova_Extended_Search_Reporting,_v16,_ c-2022-04-06.csv
2 KB

The scheduled report 'marycordova_Extended Search Reporting, v1. Search Efficiency' has

Report: marycordova_Extended Search Reporting, v1.6, Search Effi ncy

View results in Splunk

Saved Search Name	er	Efficienc	App	Host	A Runtime Secs	Weel Count	Total Runtime Secs	Ran Every X Mins	Avg Runtime In Mins
mus solar power to metric collector	s	17465.63	Kia_Ora_001	sh-i-0d220 ab6354b2f.splunktrust.splunk ud.com	3	20	34.628	504.00	0.03
Splunk Instance Restart	m ndhead	19485.79	alert_manager	sh-i-0d2202c2 354b2f.splunktrust.splunkclou om	59	12	31.038	840.00	0.04
alert_splunkd_errors	m ndhead	26924.28	ert_manager	sh-i-0d2202c2ab63 2f.splunktrust.splunkcloud.co	.87	12	22.463	840.00	0.03
mac_lookup_edit	wes	33294.80	w tys_world	sh-i-0d2202c2ab6354b plunktrust.splunkcloud.com	1.51	1	18.165	840.00	0.03
marycordova_Extended Search Reporting, v1.6, Search Efficiency	mary dova	34491.02	xpa	sh-i-0d2202c2ab6354b2f.sp ktrust.splunkcloud.com	17.54		17.535	10080.00	0.29
lookup_cloudtrail_ip_history	firebus	48852.99	firebus	sh-i-0d2202c2ab6354b2f.splun t.splunkcloud.com	12.38		12.380	10080.00	0.21
Fault Switch State Dryer	westy	63837.87	westys world	h-i-0d2202c2ab6354b2f.splunktrus lunkcloud.com	1.58	6	9.474	1680.00	0.03
Westy Wifi Node Health	westy	200530.50	westys_world	sh- st.splunkcloud.com	1.51	2	3.016	5040.00	0.03
Failure on the NAS	westy	1974.92	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	0.96	1	0.957	10080.00	0.02

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data

So What is it I Want?

- Data visibility
- Fast & easy to access
- Self-serve & on-demand
- Interactive
- Up-to-date **& fully automated**
- Nice looking
- Dynamically generated exports*
- And I **don't** want to have to work every time someone asks me for something

*Or stop doing that and just host the content somewhere

Shift Left + Law of the Instrument = 😄

Data Preparation

Use **Splunk** for data collection, normalization, and tabular formatting

This gives you a **single place to fully manage your dataset**

Data Pipeline

Use **PowerBI**® Cloud for **automated** data pipelines that are always up-to-date

Data Visualization

Use **PowerBI**® Desktop to easily create polished, **interactive**, visualizations

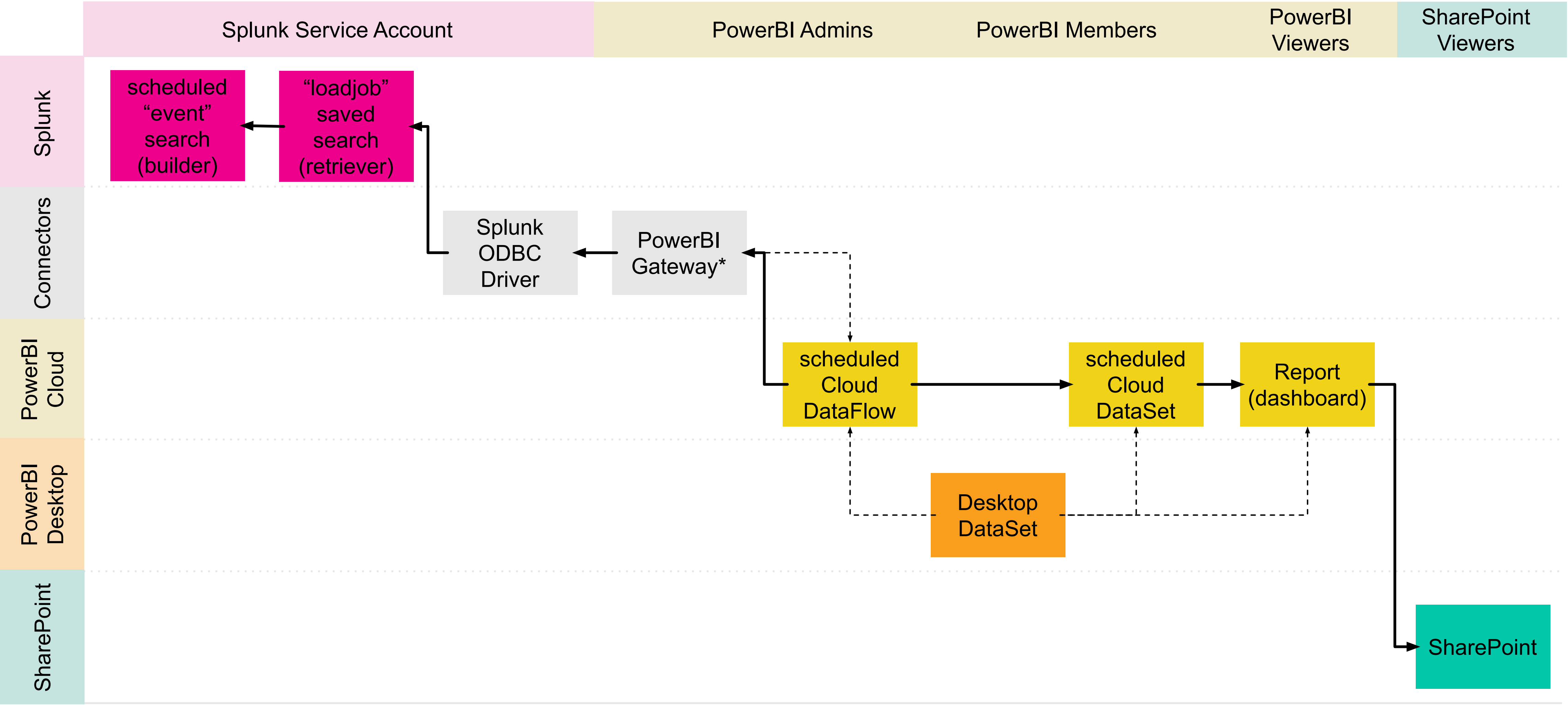
Data Distribution

Use **SharePoint** for self-serve user **access** that is interactive and enables dynamic export generation

Problems Solved!

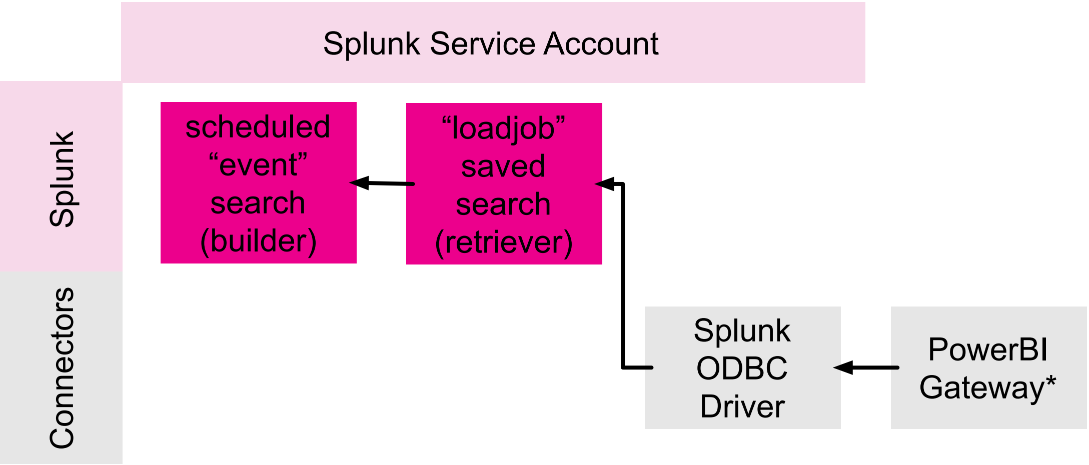
Requirement	Tool	
Visibility Fast/Easy Access Self-serve/On-demand	SharePoint	✓
Interactive Polished Dynamic Export **Automated Refresh**	PowerBI	✓
Ingestion Filtering Normalization Multivalue Expansion Tabular Formatting **Automated Refresh**	Splunk	✓

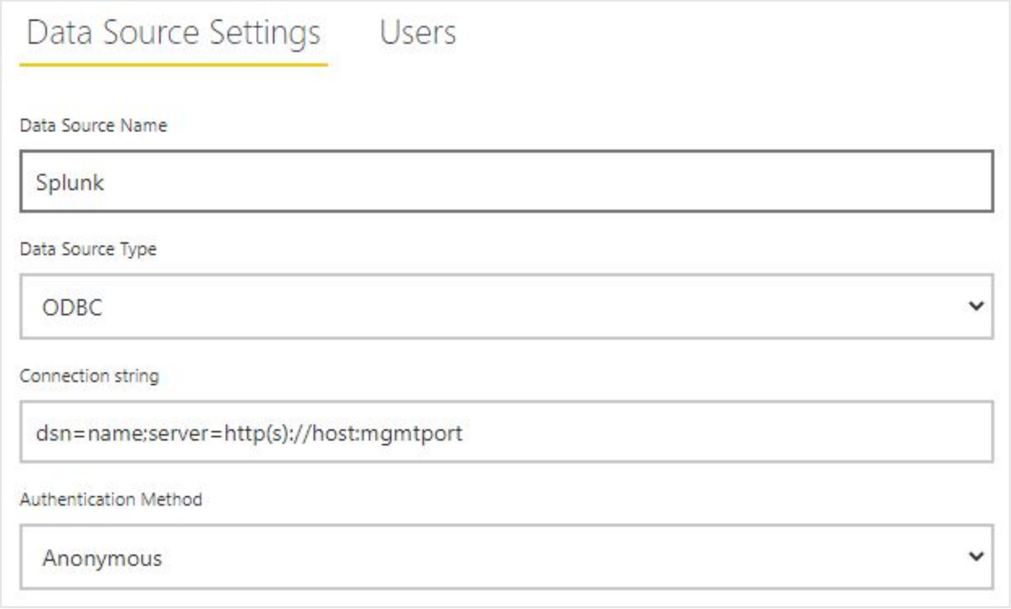
Architecture



*should probably be installed with an MS/O365 Service Account

Middleware





Data Source Name: Splunk

Data Source Type: ODBC

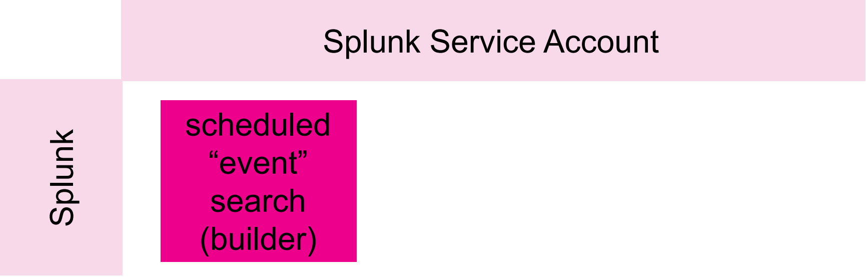
Connection string: dsn=name;server=http(s)://host:mgmtport

Authentication Method: Anonymous

- Windows
  - Network connection to Splunk http(s)://host:mgmtport
    - Splunk ODBC driver
    - Splunk service/local account
  - Network connection to PowerBI® Cloud
    - PowerBI Gateway driver
    - Probably managed by your Microsoft Admin team, otherwise easy to setup for yourself
    - Use a MS service account and not your individual credentials to register gateway driver with PowerBI Cloud
- PowerBI® Cloud Gateway
  - Add Splunk ODBC driver as a new DataSource

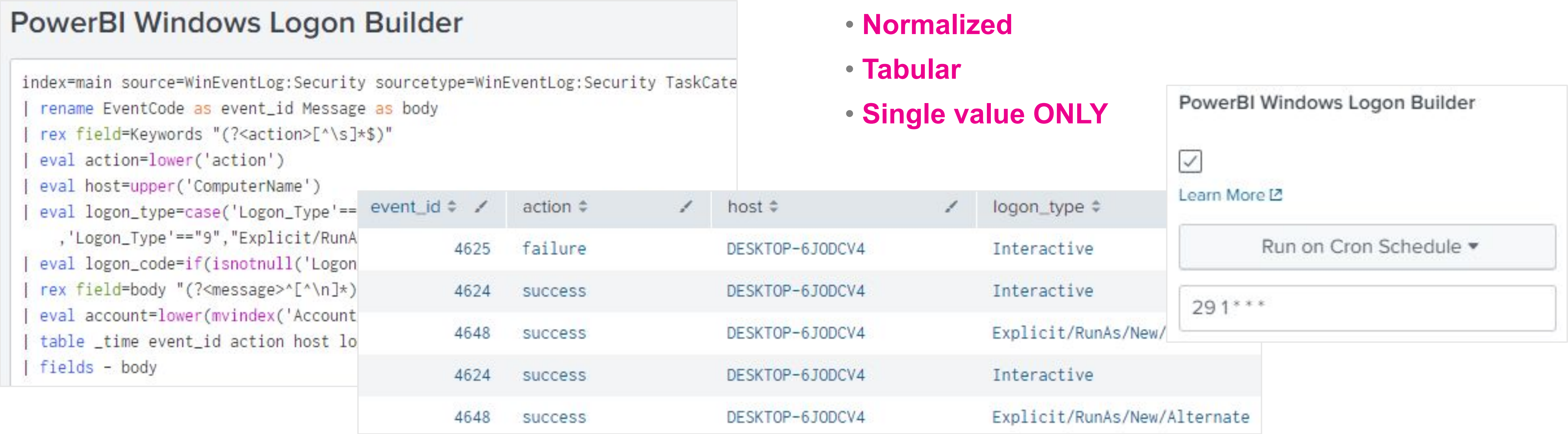
```
dsn=name;server=http(s)://host:8089
```

Splunk Builder



- Search "Builder"
  - Event search
  - Perform all you data manipulation here
  - Scheduled
  - **Normalized**
  - **Tabular**
  - **Single value ONLY**

You will have to **iterate** building your dataset, you might not know until you're already in PBI that you need to go back to Splunk.



PowerBI Windows Logon Builder

```
index=main source=WinEventLog:Security sourcetype=WinEventLog:Security TaskCate
| rename EventCode as event_id Message as body
| rex field=Keywords "(?<action>[^\s]*$)"
| eval action=lower('action')
| eval host=upper('ComputerName')
| eval logon_type=case('Logon_Type'==
   ,'Logon_Type'=="9","Explicit/RunA
| eval logon_code=if(isnotnull('Logon
| rex field=body "(?<message>^[^\n]*)
| eval account=lower(mvindex('Account
| table _time event_id action host lo
| fields - body
```

event_id	action	host	logon_type
4625	failure	DESKTOP-6JODCV4	Interactive
4624	success	DESKTOP-6JODCV4	Interactive
4648	success	DESKTOP-6JODCV4	Explicit/RunAs/New/
4624	success	DESKTOP-6JODCV4	Interactive
4648	success	DESKTOP-6JODCV4	Explicit/RunAs/New/Alternate

PowerBI Windows Logon Builder

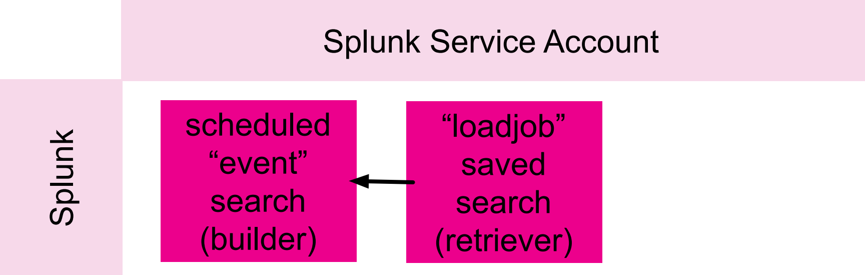
☑

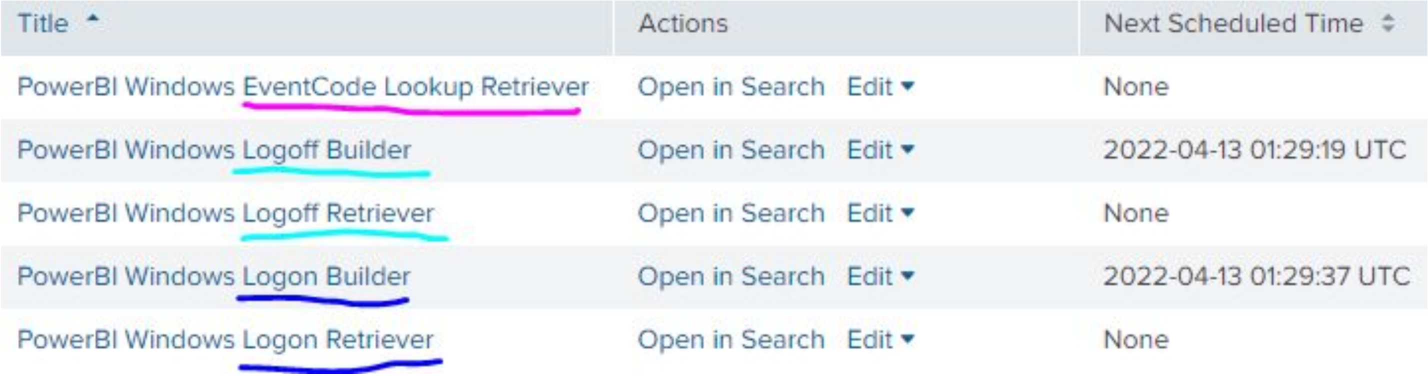
Learn More

Run on Cron Schedule ▾

29 1 * * *

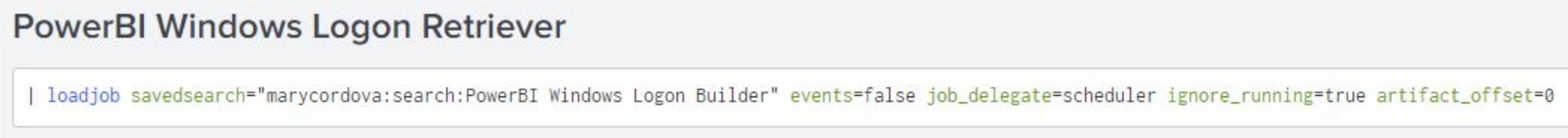
Splunk Retriever


Splunk Service Account
Splunk
scheduled "event" search (builder)
"loadjob" saved search (retriever)



Title	Actions	Next Scheduled Time
PowerBI Windows EventCode Lookup Retriever	Open in Search Edit ▾	None
PowerBI Windows Logoff Builder	Open in Search Edit ▾	2022-04-13 01:29:19 UTC
PowerBI Windows Logoff Retriever	Open in Search Edit ▾	None
PowerBI Windows Logon Builder	Open in Search Edit ▾	2022-04-13 01:29:37 UTC
PowerBI Windows Logon Retriever	Open in Search Edit ▾	None

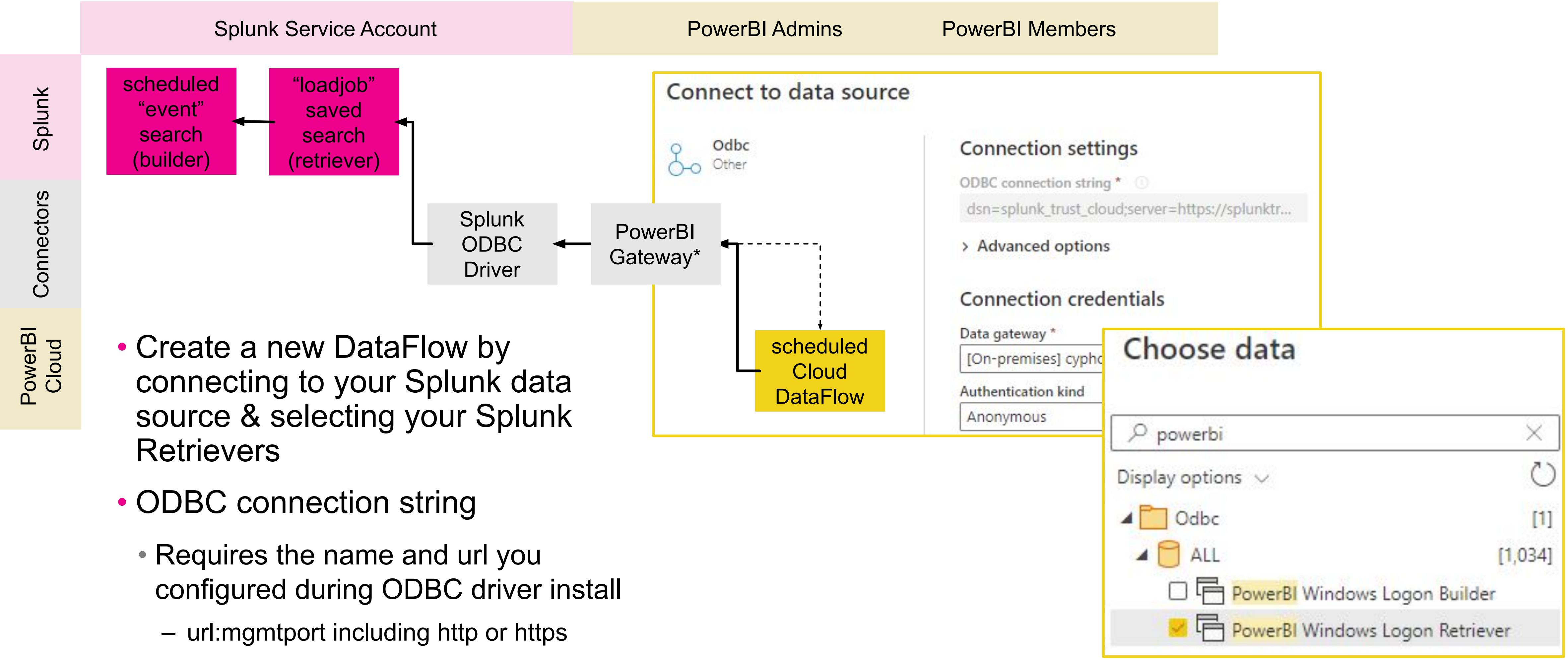
- Search "Retriever"
  - |loadjob
    - Only results
    - From the most recent, non-running
    - Corresponding scheduled Builder
  - If you need a lookup table use only a Retriever with |lookup instead
- Connect only the Retrievers to a PowerBI® Cloud DataFlow



PowerBI Windows Logon Retriever

```
| loadjob savedsearch="marycordova:search:PowerBI Windows Logon Builder" events=false job_delegate=scheduler ignore_running=true artifact_offset=0
```

PowerBI® Cloud DataFlow



Connect to data source

Odbc
Other

Connection settings

ODBC connection string *
dsn=splunk_trust_cloud;server=https://splunktr...

› Advanced options

Connection credentials

Data gateway *
[On-premises] cypho

Authentication kind
Anonymous

Choose data

powerbi

Display options

◢ Odbc [1]
◢ ALL [1,034]
☐ PowerBI Windows Logon Builder
☑ PowerBI Windows Logon Retriever

- Create a new DataFlow by connecting to your Splunk data source & selecting your Splunk Retrievers
- ODBC connection string
  - Requires the name and url you configured during ODBC driver install
    - url:mgmtport including http or https

```
dsn=name;server=http(s)://host:8089
```

PowerBI® Cloud DataFlow

- **Do not do any data manipulation here**
  - You will be tempted
  - Go back to Splunk instead
- DataFlow
  - Bundle your Splunk reports logically
- **Automated** refresh
  - Schedule to start after you are sure your Splunk refreshes are complete

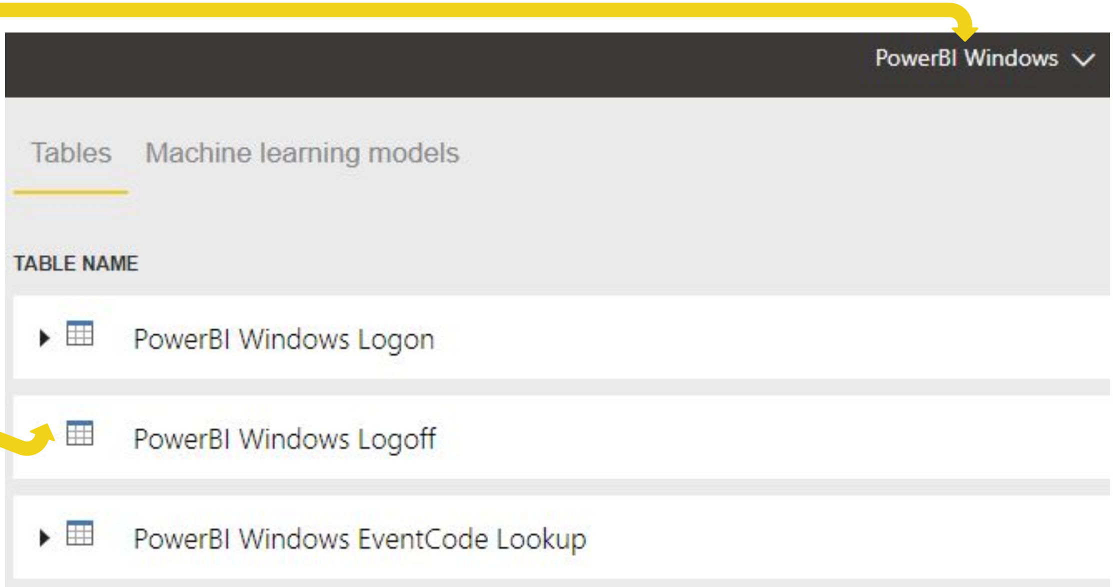
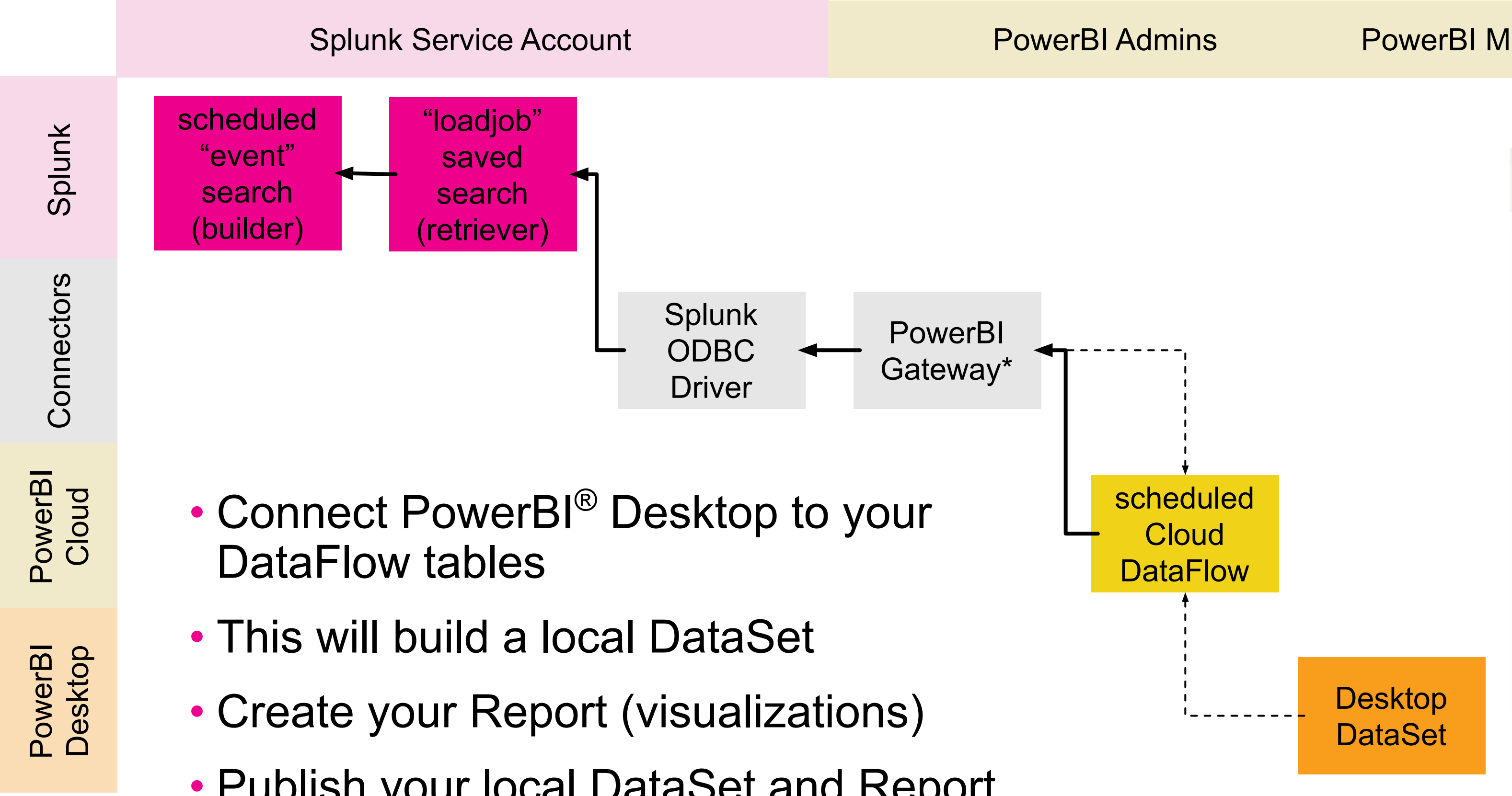


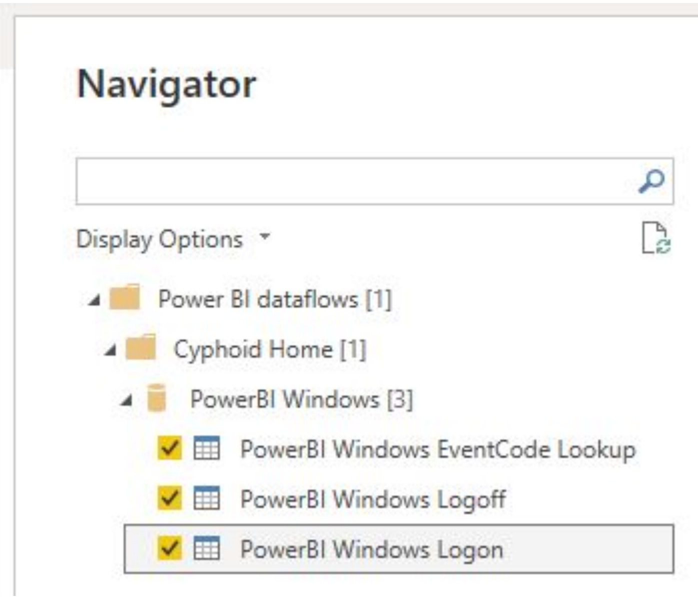
TABLE NAME

- PowerBI Windows Logon
- PowerBI Windows Logoff
- PowerBI Windows EventCode Lookup

PowerBI® Desktop



- Connect PowerBI® Desktop to your DataFlow tables
- This will build a local DataSet
- Create your Report (visualizations)
- Publish your local DataSet and Report back to PowerBI® Cloud and schedule an automated refresh



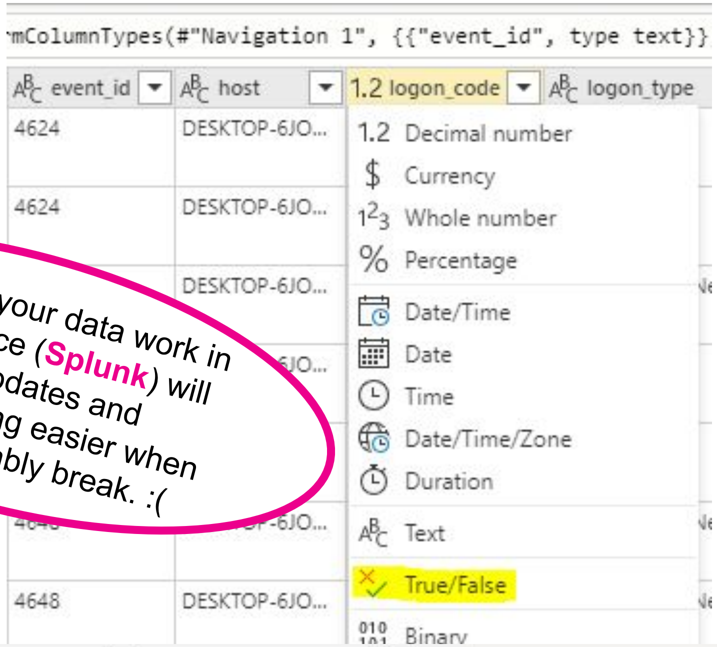
☑ PowerBI Windows EventCode Lookup
☑ PowerBI Windows Logoff
☑ PowerBI Windows Logon

Publishing to Power BI

Publishing 'PowerBI Windows.pbix' to Power BI

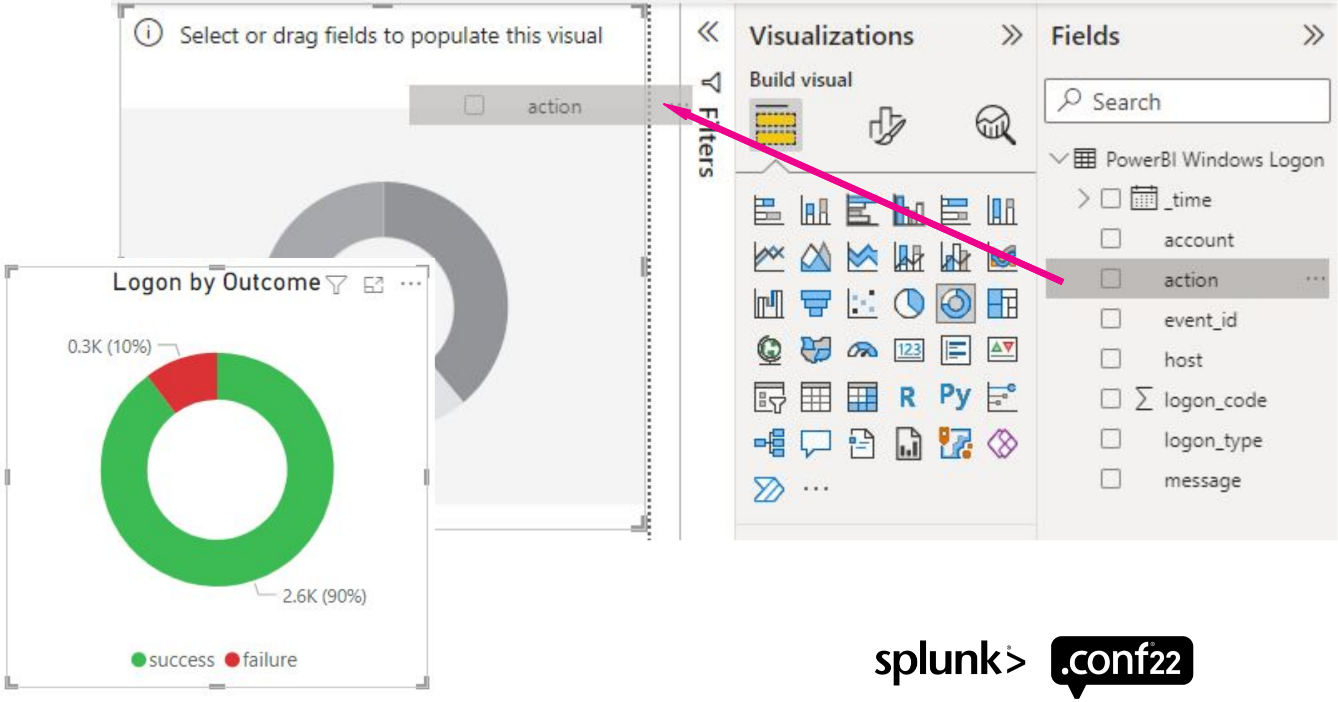
PowerBI® Desktop

- **Do not do any data manipulation here**
  - You will be tempted
  - Go back to Splunk instead
- DataSets
  - If you must, you can make small data changes that are specific to PowerBI, such as data types
    - – numeric to text, etc
- Reports
  - Quickly and easily drag and drop visualizations onto your cleaned and prepared Splunk data
- Publishing
  - Send it all back to the cloud for **automated** refresh and sharing
    - – Schedule the refresh to occur after the DataFlow refresh has completed

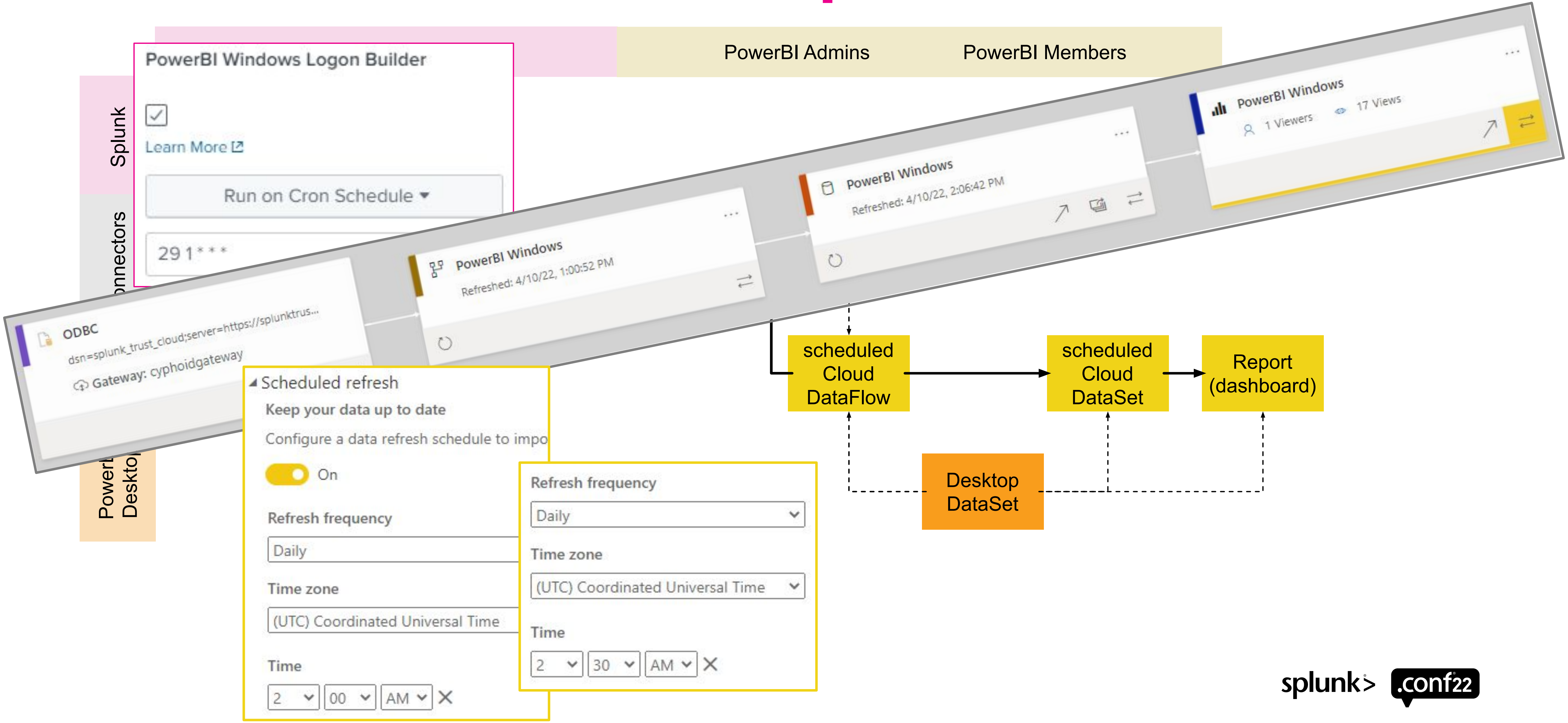


```
mColumnTypes(#"Navigation 1", {{"event_id", type text}}
```

Keeping all your data work in a single place (**Splunk**) will make updates and troubleshooting easier when things inevitably break. :(



Automated Refresh Pipeline



PowerBI Windows Logon Builder

☑

Learn More

Run on Cron Schedule ▾

29 1 * * *

ODBC

dsn=splunk_trust_cloud;server=https://splunktrus...

Gateway: cyphoidgateway

PowerBI Windows

Refreshed: 4/10/22, 1:00:52 PM

PowerBI Windows

Refreshed: 4/10/22, 2:06:42 PM

PowerBI Windows

1 Viewers 17 Views

Scheduled refresh

Keep your data up to date

Configure a data refresh schedule to impo

● On

Refresh frequency: Daily

Time zone: (UTC) Coordinated Universal Time

Time: 2 00 AM

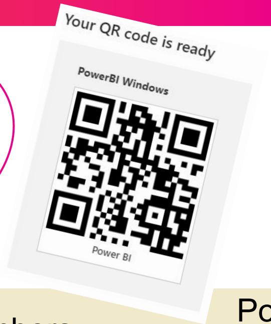
Refresh frequency: Daily

Time zone: (UTC) Coordinated Universal Time

Time: 2 30 AM

SharePoint

Maybe embed QR codes in email! 🤯



Splunk Service Account | PowerBI Admins | PowerBI Members | PowerBI Viewers | SharePoint Viewers

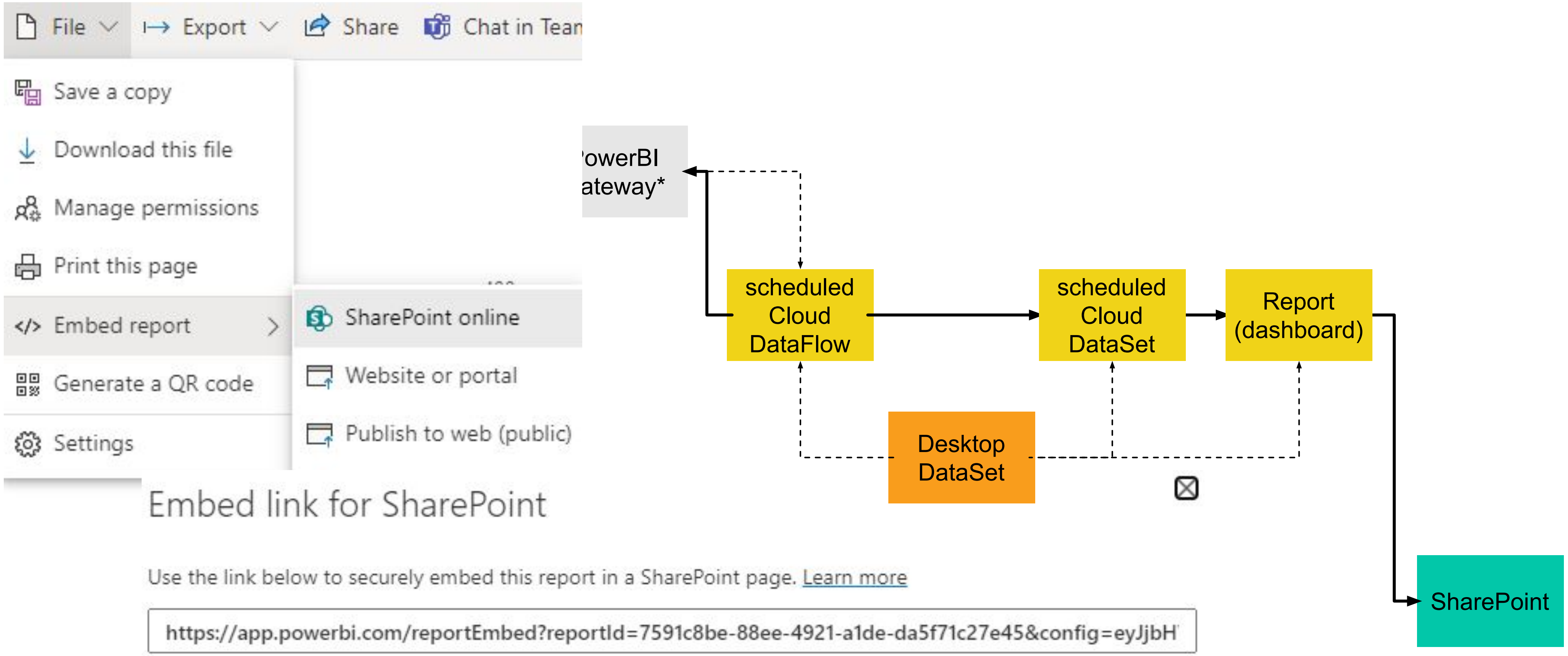
Splunk

Connectors

PowerBI Cloud

PowerBI Desktop

SharePoint



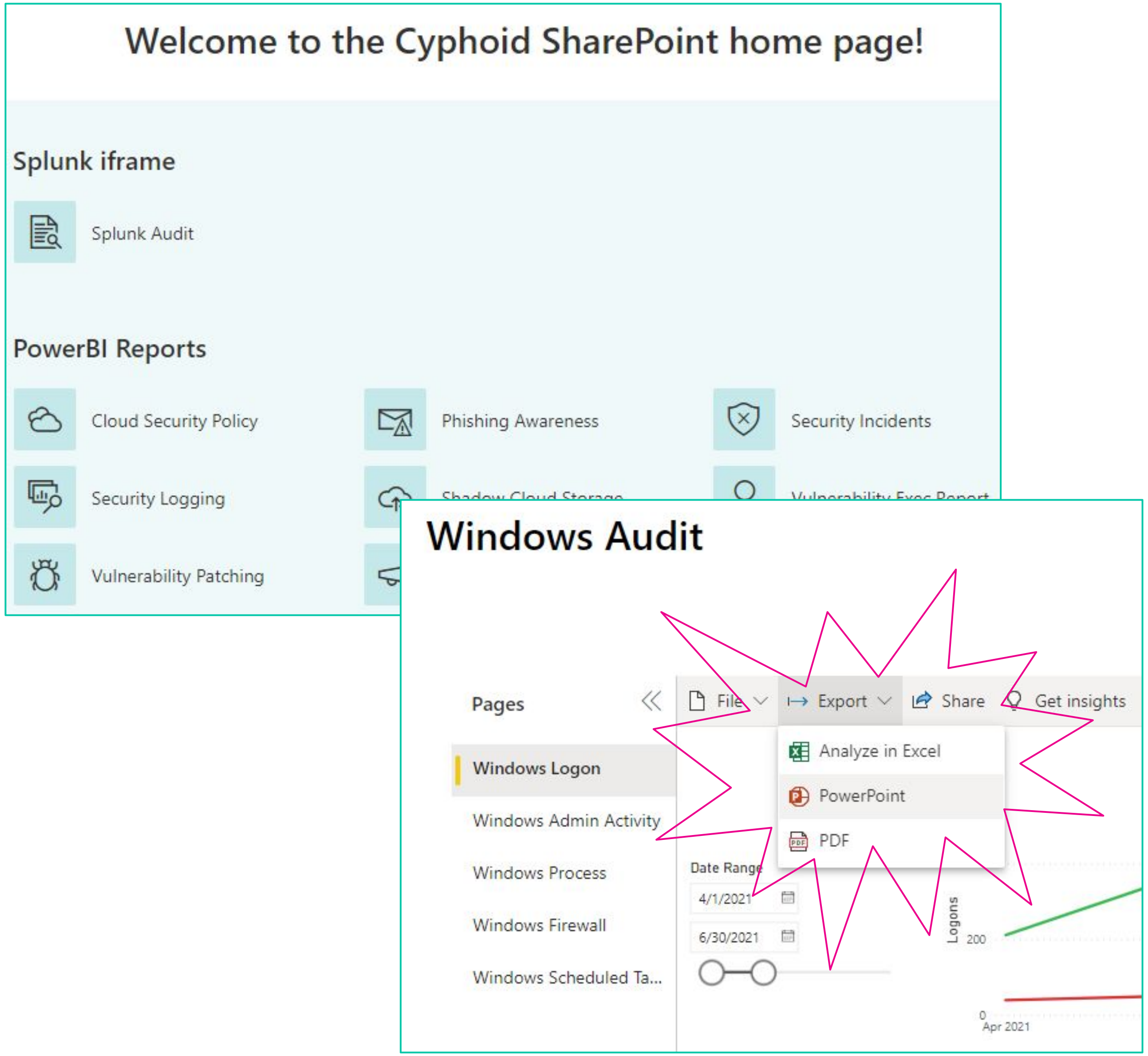
Embed link for SharePoint

Use the link below to securely embed this report in a SharePoint page. Learn more

https://app.powerbi.com/reportEmbed?reportId=7591c8be-88ee-4921-a1de-da5f71c27e45&config=eyJjbH

SharePoint

- Users probably already use it daily
- SharePoint enables:
  - One place for a **diverse** group **stakeholders** to **access** reports/dashboards
  - An **easy** login experience (hopefully YMMV)
  - Intuitive and navigable sites (if you build it that way)
  - Access to the **dynamic/interactive sorting** and **filtering** of PowerBI
  - Access to the customized exports of PowerBI
  - Ability to **stop exporting** and **start sharing**
    - – Just screenshare, or grant access to the reports instead



Welcome to the Cyphoid SharePoint home page!

Splunk iframe

Splunk Audit

PowerBI Reports

Cloud Security Policy

Phishing Awareness

Security Incidents

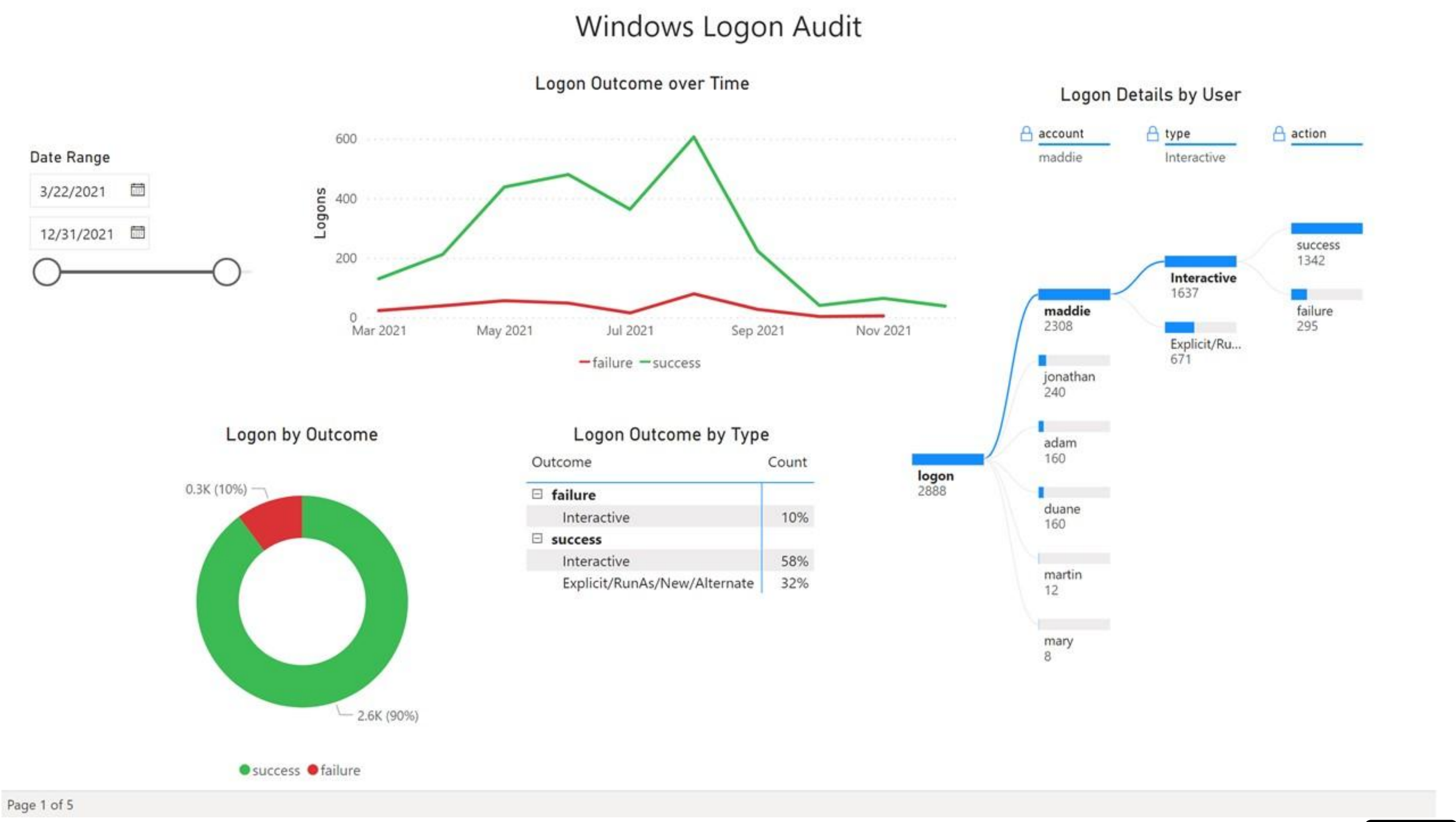
Security Logging

Shadow Cloud Storage

Vulnerability Exec Report

Vulnerability Patching

Windows Audit



Windows Logon Audit

Date Range

3/22/2021

12/31/2021

Logon Outcome by Type

Outcome	Count
⊟ **failure**	
Interactive	10%
⊟ **success**	
Interactive	58%
Explicit/RunAs/New/Alternate	32%

Page 1 of 5

Access Control

- Splunk service account constrained to a specific App
  - Connectors & DataFlows can only access saved Reports/Alerts in that App
- Only PowerBI® Gateway and PowerBI® ODBC Driver DataSource Admins can create or modify a DataFlow
- Only PowerBI® Workspace Members can use a DataFlow to create or modify a DataSet & Report
- Provision users with View access to your PowerBI® Workspace and SharePoint site
  - Everyone will need PowerBI Pro license
    - Included in E5 or $10 per user per month

Thank You

splunk> .conf22