

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.

Splunk, Splunk> and Turn Data Into Doing 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. © 2022 Splunk Inc. All rights reserved.

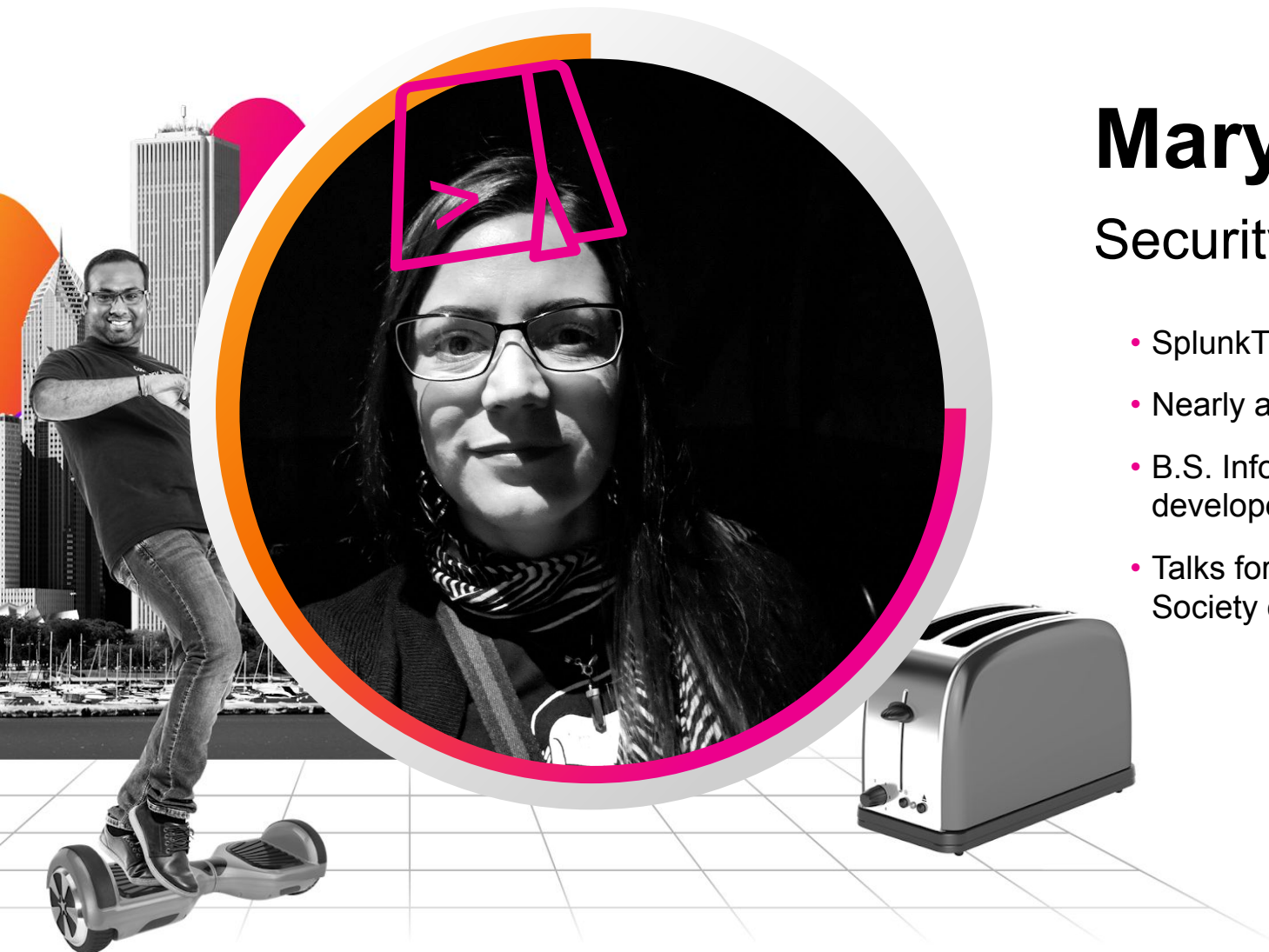
Dynamic Splunk Data Delivered Where Your Executives Live

PLA1122B

Mary Cordova
Security Operations



splunk> .conf22



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, ISC² exam developer, CompTIA A+
- Talks for Splunk .conf® & User Groups, Shellcon, Women's Society of Cyberjutsu, San Diego DFIR Meetup

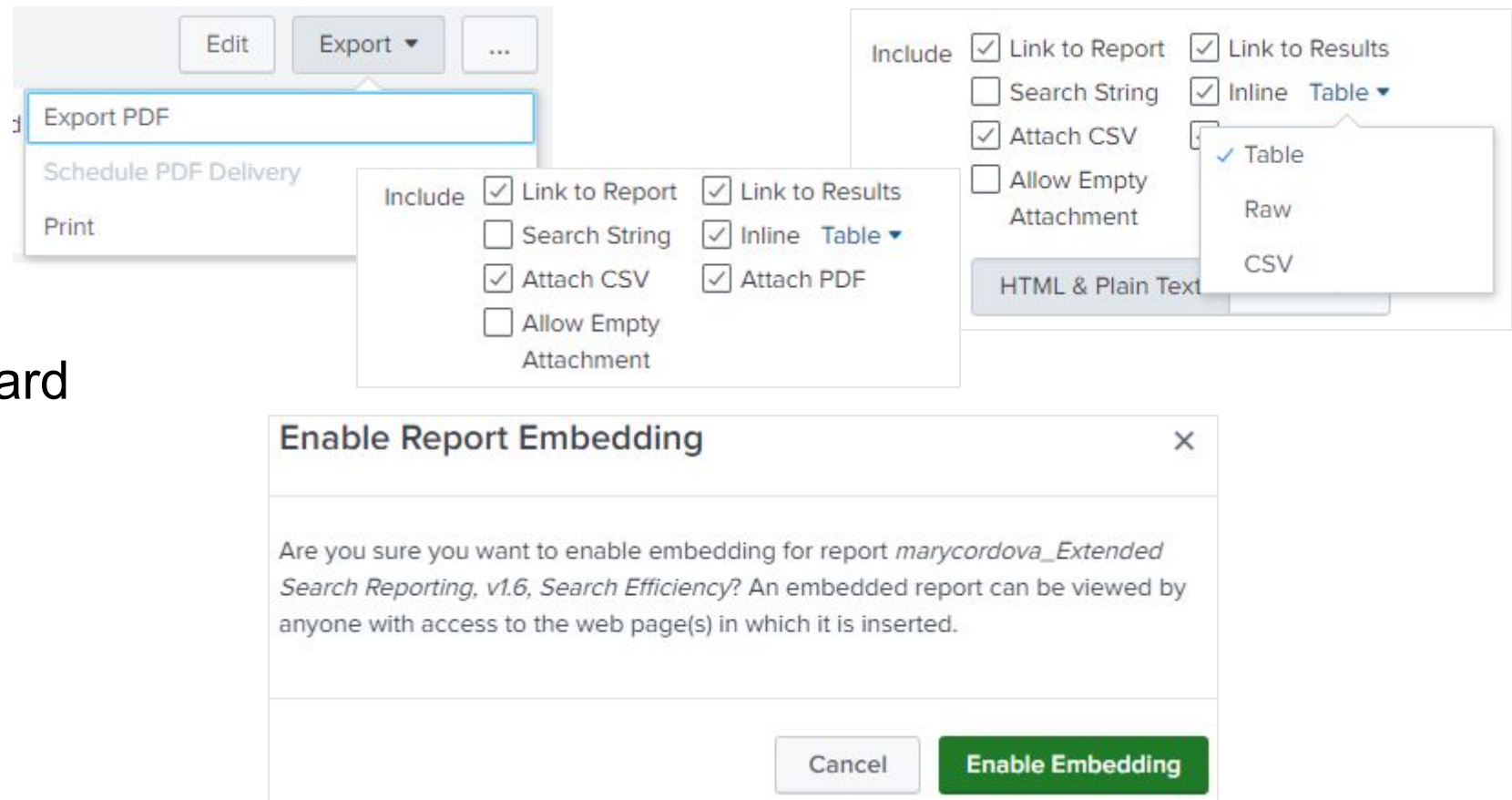
Why Not Use Splunk for Everything?

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** 😞

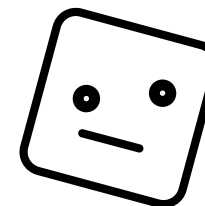
What Options* Did I Look Into?

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



*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

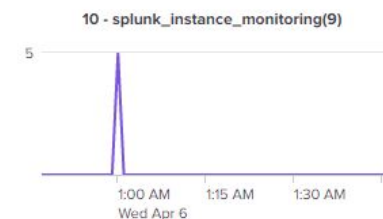
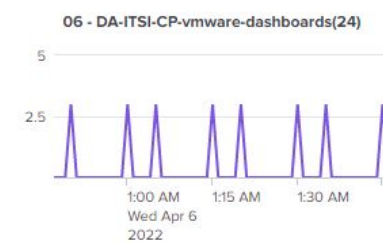
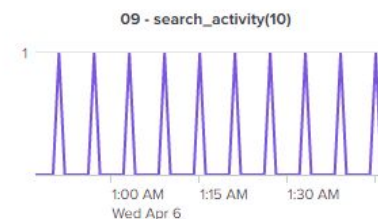
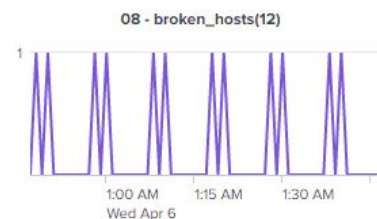
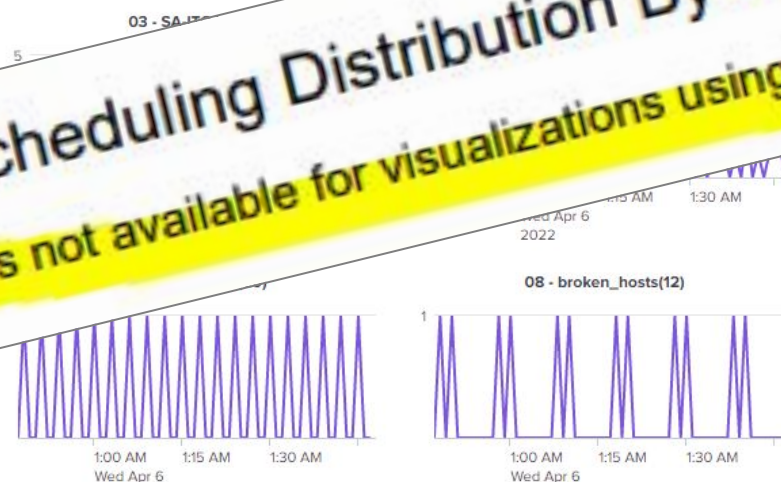
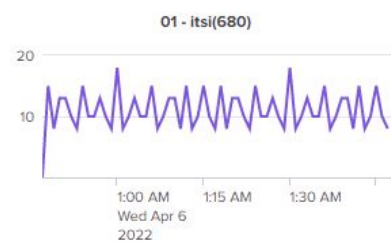
Select timechart span

Custom time

☒ 1 minute

☐ 5 minutes

☐ 60 minutes

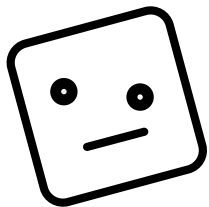


Search Scheduling Distribution By App

PDF export is not available for visualizations using trellis layout.

Dashboard Export

Saved Search Name ↕	User ↕	Efficiency ↕	App ↕	Host ↕
mus solar power to metric collector	mus	16601.70	Kia_Ora_001	sh-i-0d2202c2ab6354b2f.spl
Splunk Instance Restart	my2ndhead	21273.30	alert_manager	sh-i-0d2202c2ab6354b2f.sp
alert_splunkd_errors	my2ndhead	27578.66	alert_manager	sh-i-0d2202c2ab6354b2f.?
mac_lookup_edit	westy	30680.26	westys_world	sh-i-0d2202c2ab6354b2f
Westy Wifi Node Health	westy	46764.09	westys_world	sh-i-0d2202c2ab6354b2
lookup_cloudtrail_ip_history	firebus	54217.84	firebus	sh-i-0d2202c2ab6354b
Fault_Switch_State_Dryer	westy	61916.46	westys_world	sh-i-0d2202c2ab6354
Failure on the NAS	westy	617142.86	westys_world	sh-i-0d2202c2ab63f



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	6.47	2	12.933
5	Westy Wifi Node Health	westy	46764.09	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.63	6	9.768
6	lookup_cloudtrail_ip_history	firebus	54217.84	firebus	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	0.98	1	0.980
7	Fault_Switch_State_Dryer	westy	61916.46	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com			
8	Failure on the NAS	westy	617142.86	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com			

Mins ↕	Avg Runtime In Mins ↕
504.00	0.03
840.00	0.04
840.00	0.03
840.00	0.03
5040.00	0.11
10080.00	0.19
1680.00	0.03
10080.00	0.02

splunk>

Extended Search Reporting, v1.6

2022-04-06 01:53:21 UTC
Page 1

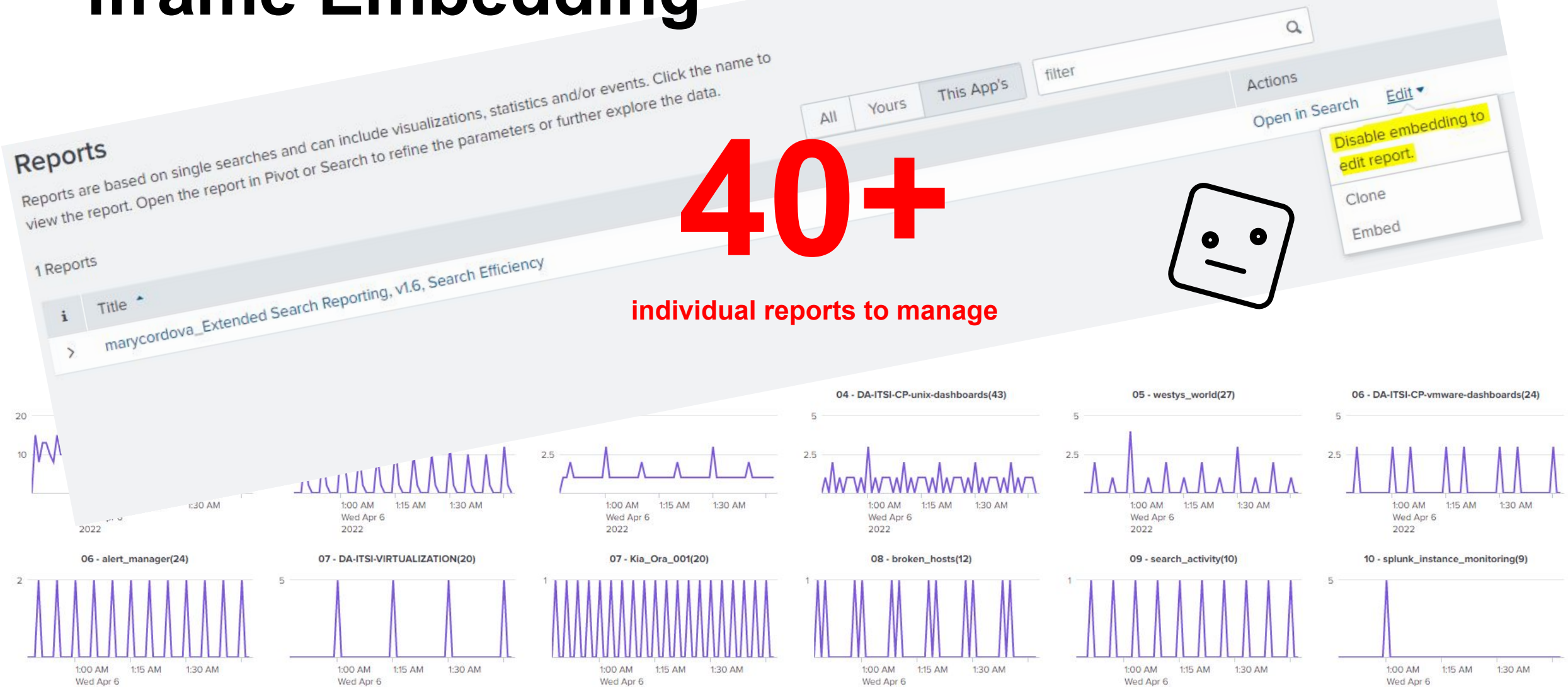
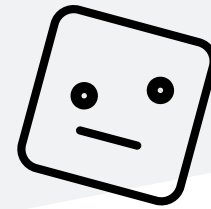
Efficiency Search (Columns 9-10 of 10)

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

iframe Embedding

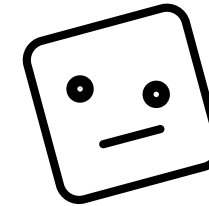
40+

individual reports to manage



iframe Embedding

Report not available.



Efficiency Search

Exclusions

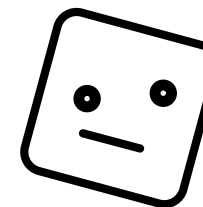
- ☒ Exclude Accelerations
- ☒ Searches not owned by admin
- ☒ Searches not owned by nobody

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



Saved Search Name	User	Efficiency	App	Host	Avg Runtime Secs	Weekly Count	Total Runtime Secs	Ran Every X Mins
mus solar power to metric collector	mus	8846.63	xpac	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	2.85	24	68.365	420.00
Splunk Instance Restart	my2ndhead	18217.96	Kia_Ora_001	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.66	20	33.198	504.00
collector	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, Search 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 browser.



marycordova_Extended_Search_Reporting_v16_Searc-2022-04-06.pdf
10 KB



marycordova_Extended_Search_Reporting_v16_Searc-2022-04-06.csv
2 KB

The scheduled report 'marycordova_Extended Search Reporting, v1.6, Search Efficiency' has been generated.

Report: [marycordova_Extended Search Reporting, v1.6, Search Efficiency](#)

[View results in Splunk](#)

Saved Search Name	Owner	Efficiency	App	Host	Alert	Runtime Secs	Week Count	Total Runtime Secs	Ran Every X Mins	Avg Runtime In Mins
mus solar power to metric collector	ms	17465.63	Kia_Ora_001	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.83	20	1	34.628	504.00	0.03
Splunk Instance Restart	marycordova	19485.79	alert_manager	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.59	12	1	31.038	840.00	0.04
alert_splunkd_errors	marycordova	26924.28	alert_manager	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.87	12	1	22.463	840.00	0.03
mac_lookup_edit	westy	33294.80	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.51	17	1	18.165	840.00	0.03
marycordova_Extended Search Reporting, v1.6, Search Efficiency	marycordova	34491.02	xpac	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	17.54	1	1	17.535	10080.00	0.29
lookup_cloudtrail_ip_history	firebus	48852.99	firebus	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	12.38	1	1	12.380	10080.00	0.21
Fault Switch State Dryer	westy	63837.87	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.58	6	1	9.474	1680.00	0.03
Westy Wifi Node Health	westy	200530.50	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	1.51	2	1	3.016	5040.00	0.03
Failure on the NAS	westy	1974.92	westys_world	sh-i-0d2202c2ab6354b2f.splunktrust.splunkcloud.com	0.96	1	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



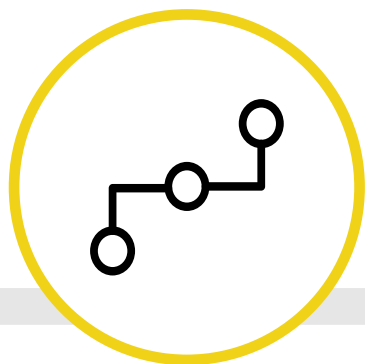
Shift Left + Law of the Instrument =



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

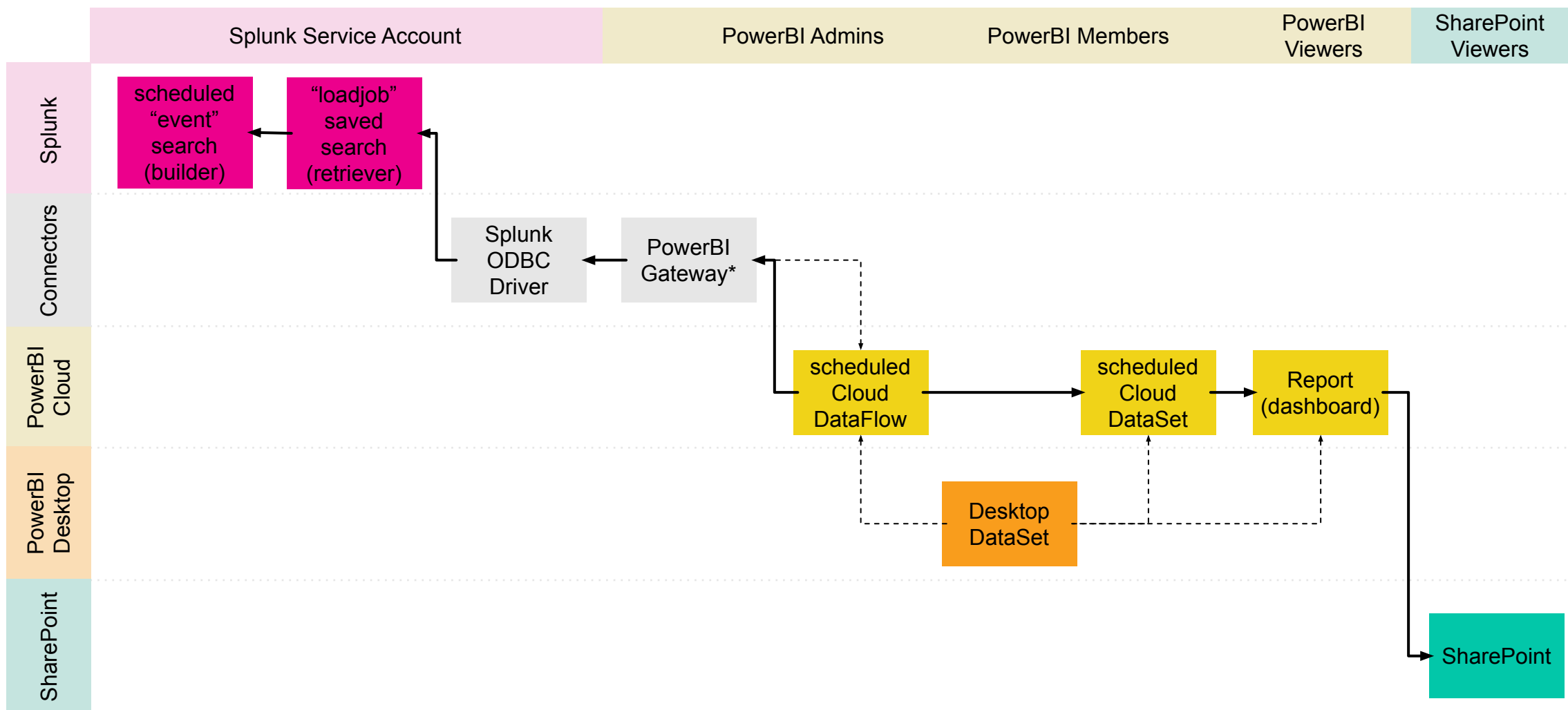


Ingestion
Filtering
Normalization
Multivalue Expansion
Tabular Formatting
Automated Refresh

Splunk

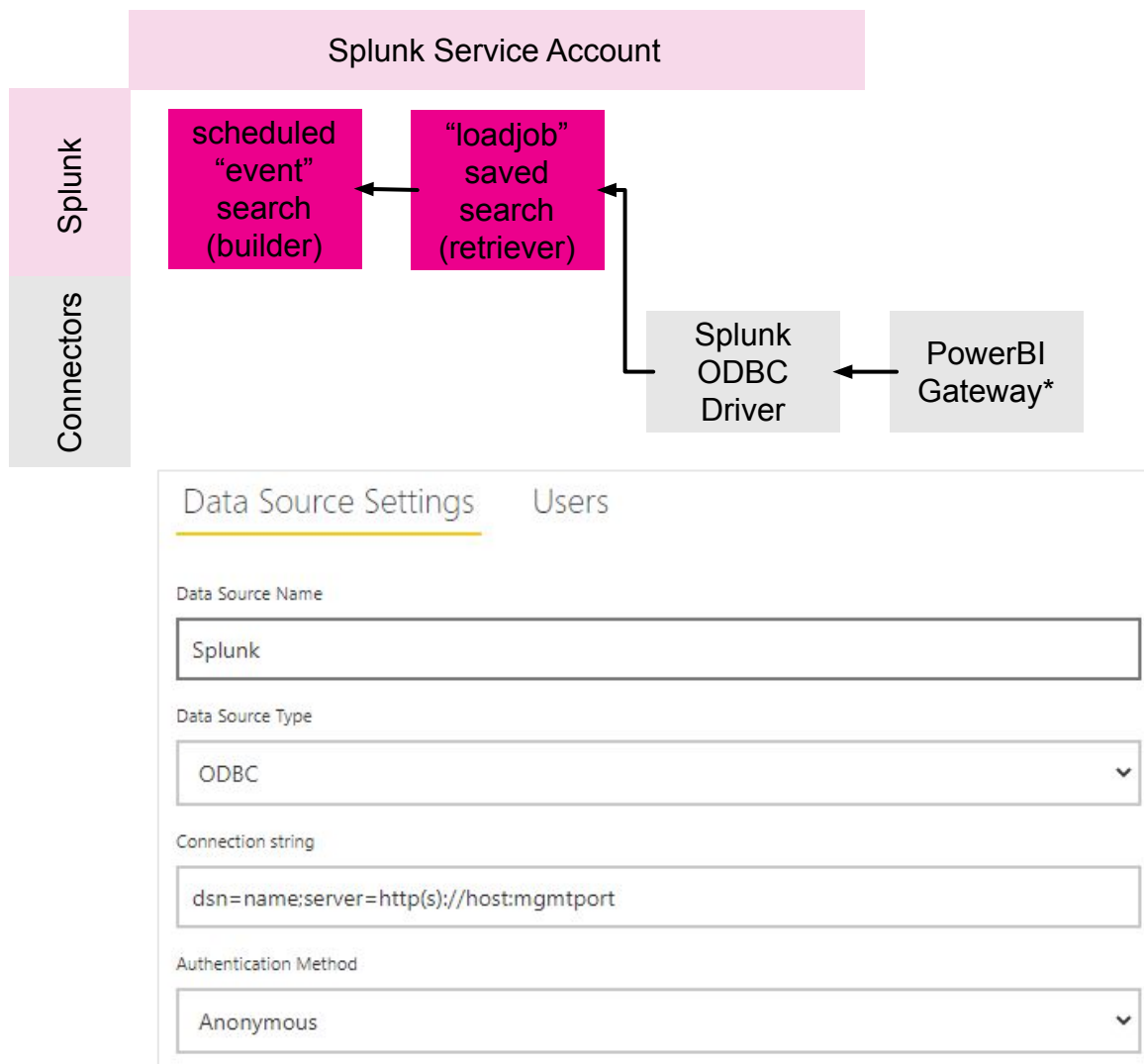


Architecture



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

Middleware



• Windows

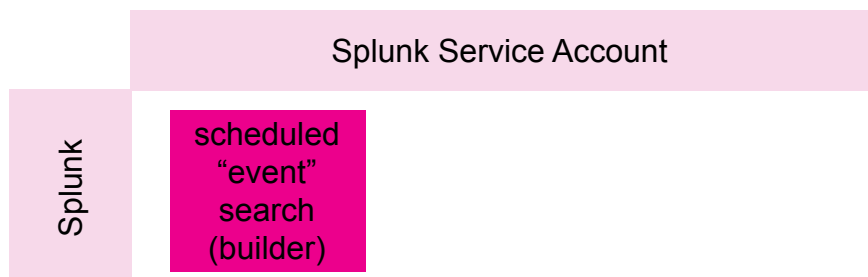
- Network connection to Splunk `http(s)://host:mgmtport`
 - [Splunk ODBC driver](#)
 - Splunk service/local account
- Network connection to PowerBI® Cloud
 - [PowerBI Gateway driver](#)
 - Probably managed by your Microsoft Admin team, otherwise easy to setup for yourself
 - Use a MS service account 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



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

• 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

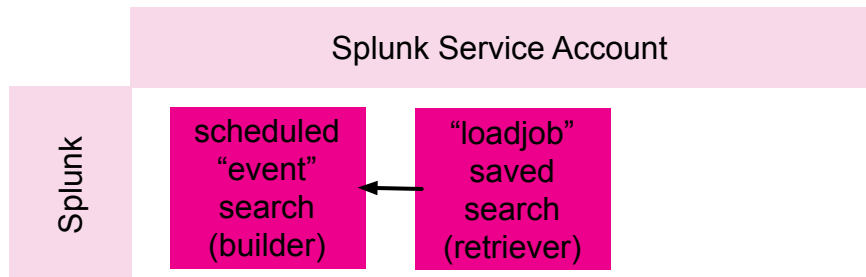


[Learn More](#)

Run on Cron Schedule ▼

29 1 * * *

Splunk Retriever



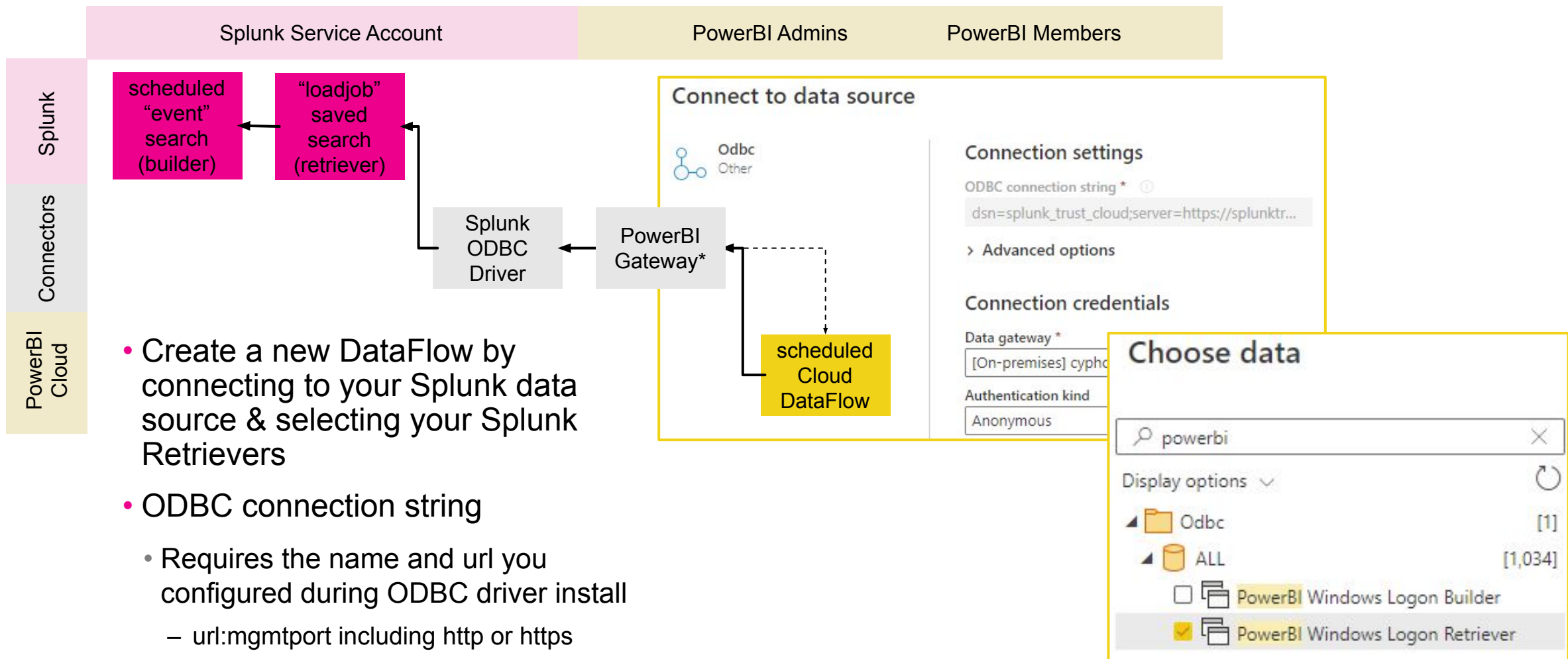
Title	Actions	Next Scheduled Time
PowerBI Windows <u>EventCode Lookup Retriever</u>	Open in Search Edit ▼	None
PowerBI Windows <u>Logoff Builder</u>	Open in Search Edit ▼	2022-04-13 01:29:19 UTC
PowerBI Windows <u>Logoff Retriever</u>	Open in Search Edit ▼	None
PowerBI Windows <u>Logon Builder</u>	Open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

PowerBI Windows Logon Retriever

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

- 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® Cloud DataFlow



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

PowerBI® Cloud DataFlow

- **Do not do any data manipulation here**

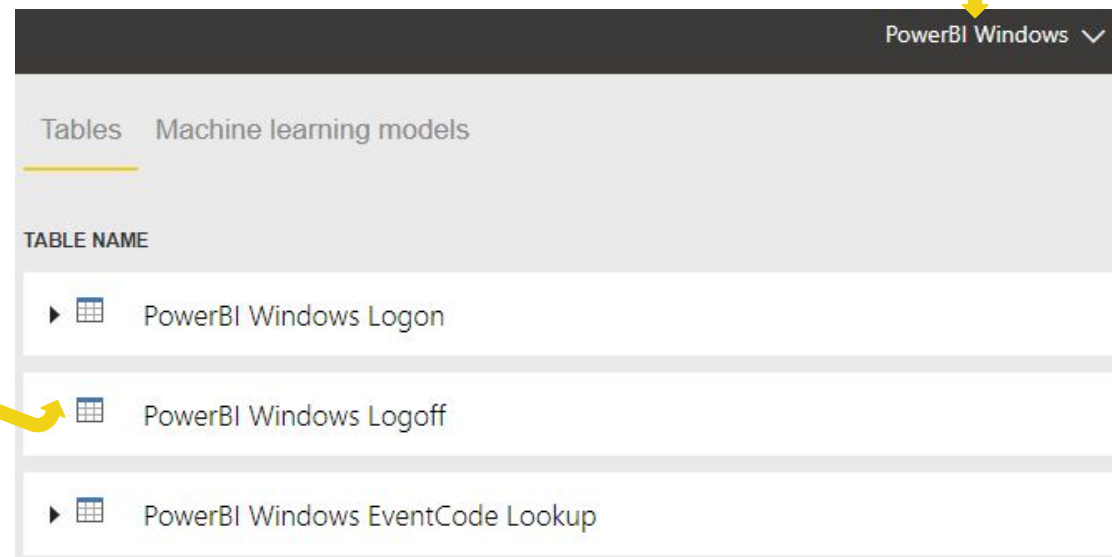
- You will be tempted
- Go back to Splunk instead

- DataFlow

- Bundle your Splunk reports logically

- **Automated** refresh

- Schedule to start after you are sure your Splunk refreshes are complete



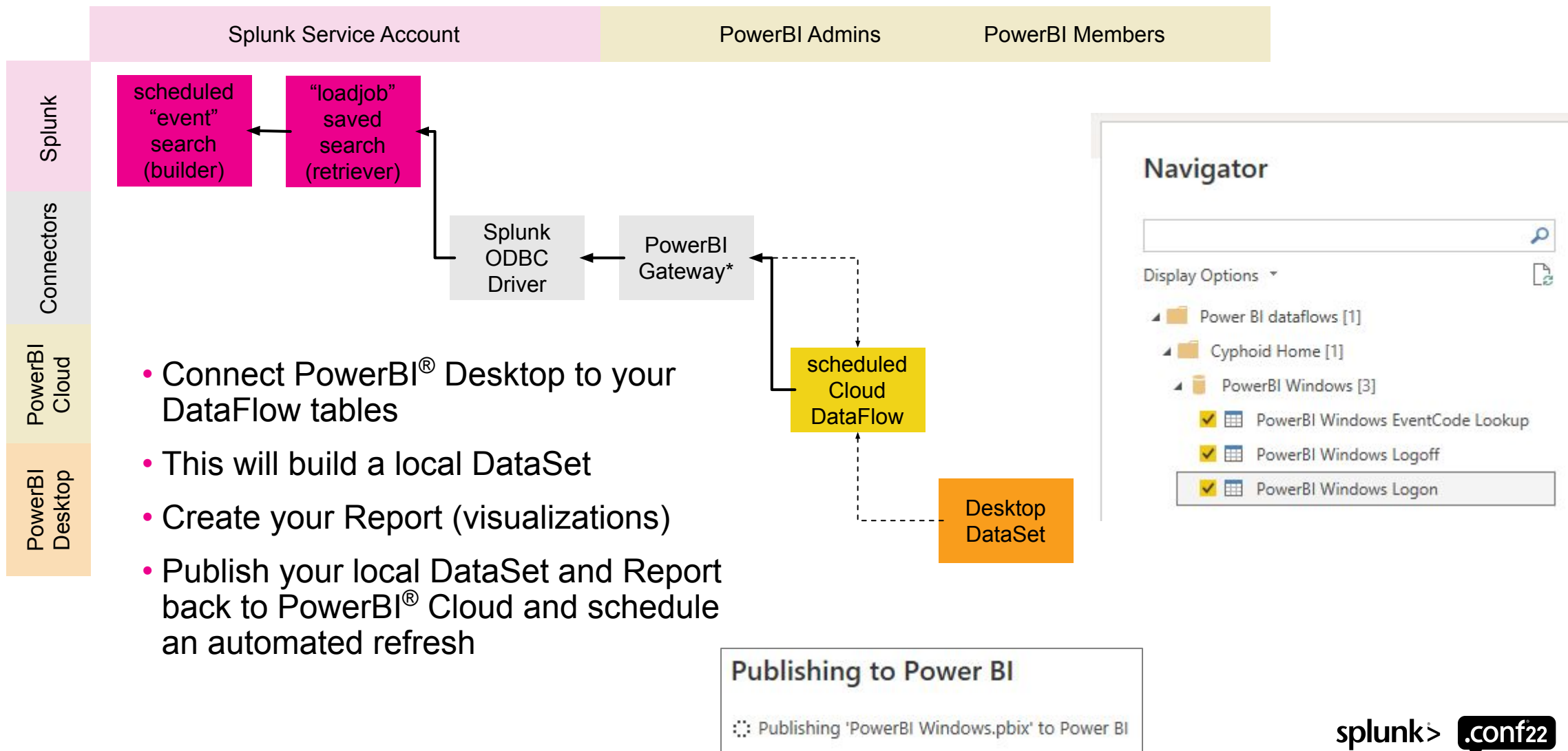
PowerBI Windows ▾

Tables Machine learning models

TABLE NAME

▶	PowerBI Windows Logon
▶	PowerBI Windows Logoff
▶	PowerBI Windows EventCode Lookup

PowerBI® Desktop



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

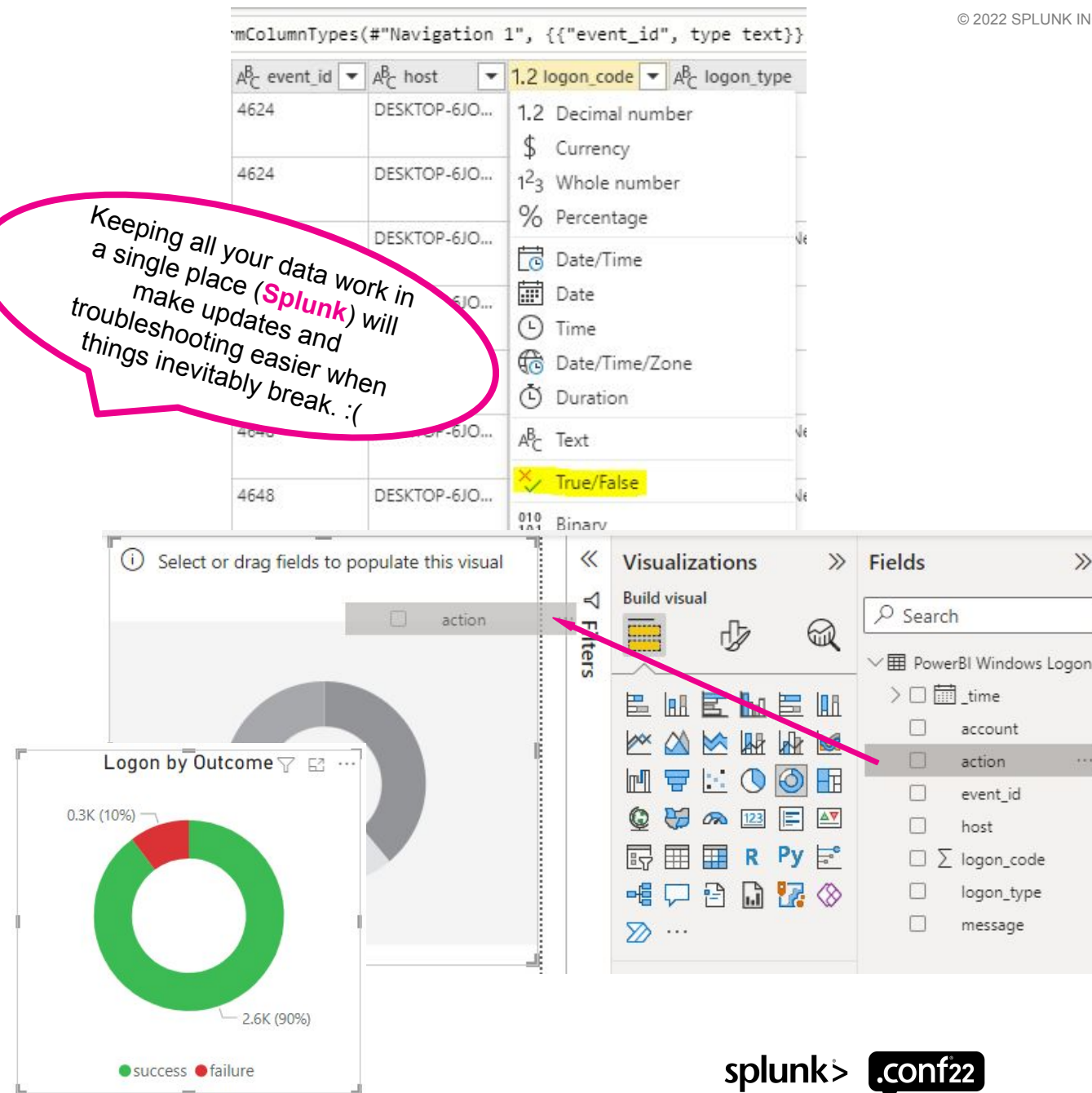
- Reports

- Quickly and easily drag and drop visualizations onto your cleaned and prepared Splunk data

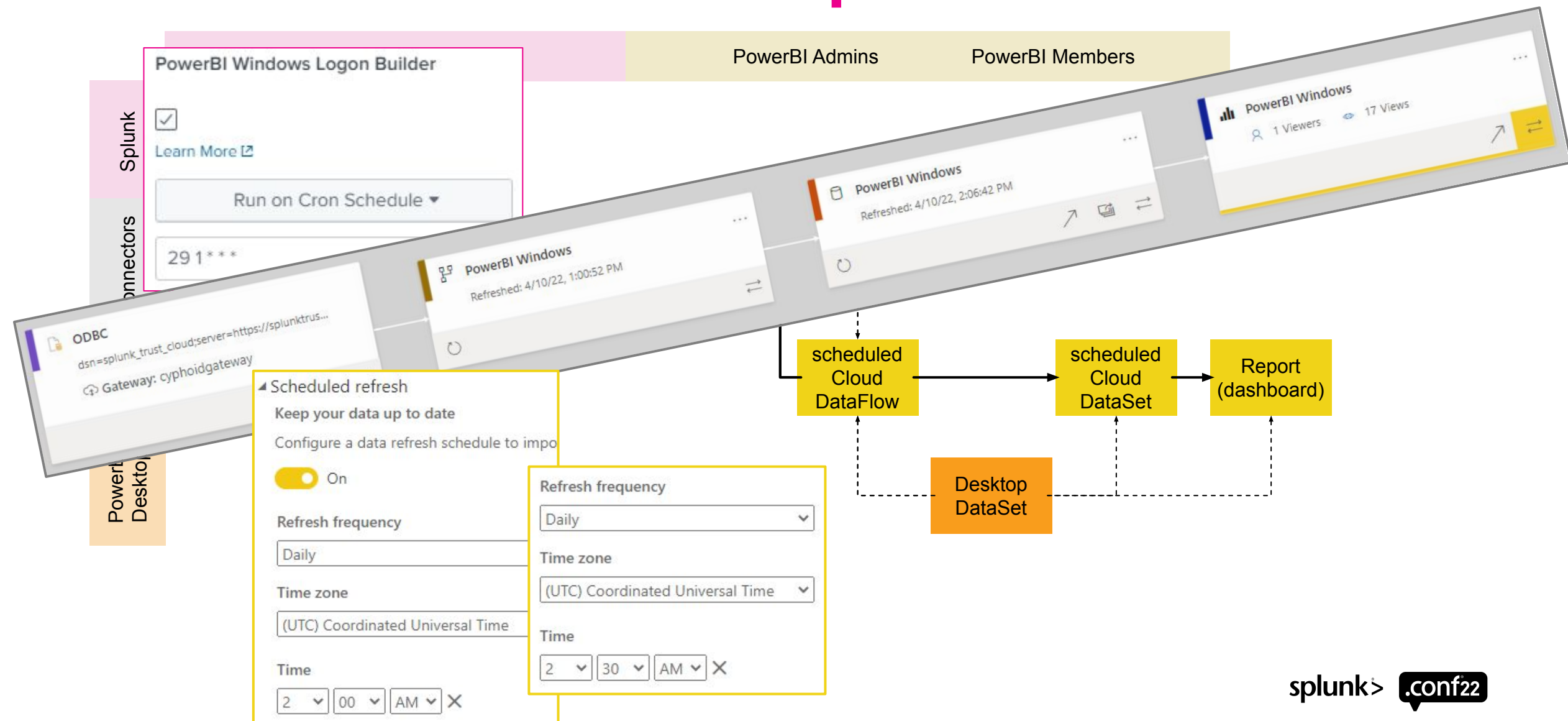
- Publishing

- Send it all back to the cloud for **automated** refresh and sharing
 - Schedule the refresh to occur after the DataFlow refresh has completed

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

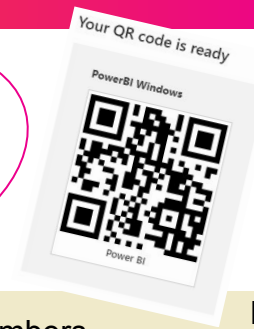


Automated Refresh Pipeline



SharePoint

Maybe
embed QR
codes in
email! 🤖



Splunk Service Account

PowerBI Admins

PowerBI Members

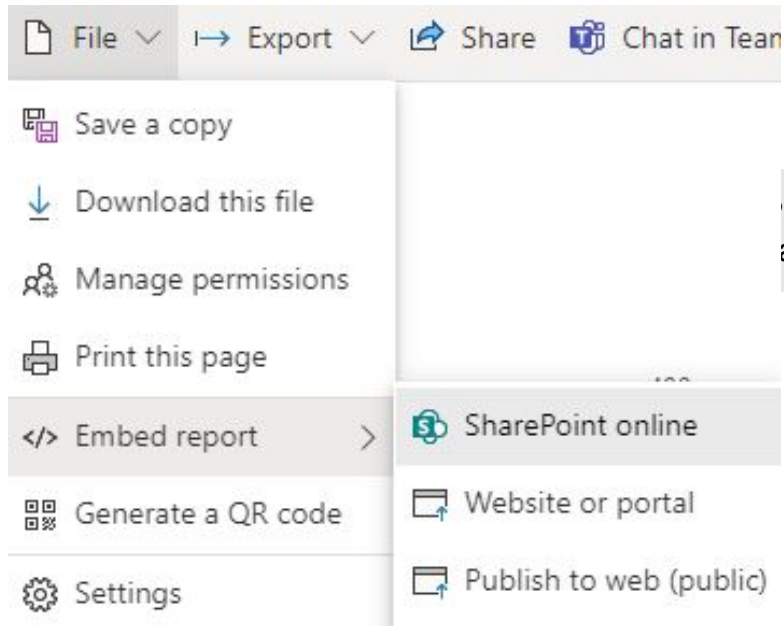
PowerBI
ViewersSharePoint
Viewers

Splunk

Connectors

PowerBI
CloudPowerBI
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>

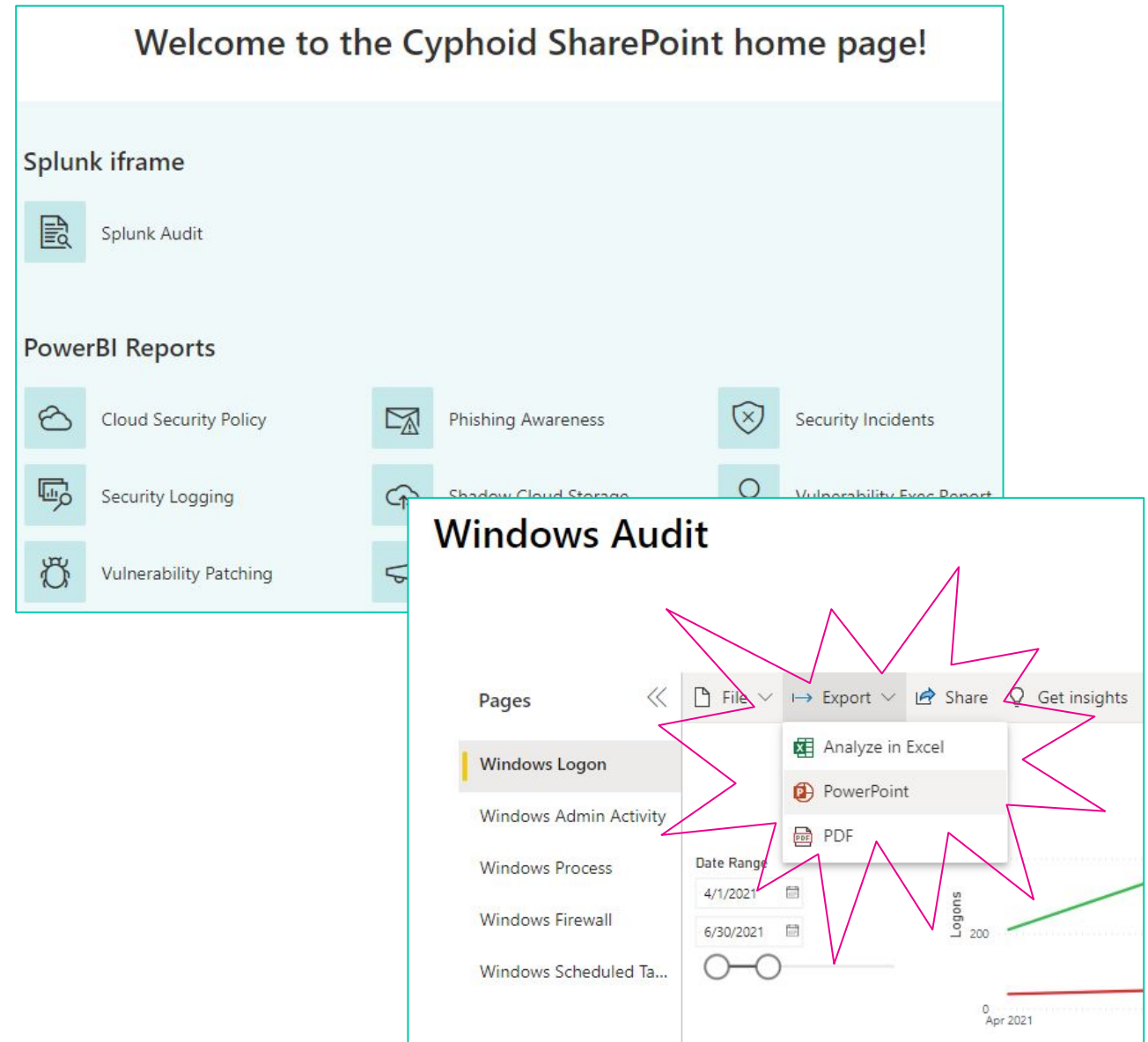
PowerBI
gateway*scheduled
Cloud
DataFlowscheduled
Cloud
DataSetReport
(dashboard)Desktop
DataSet

SharePoint

splunk> .conf22

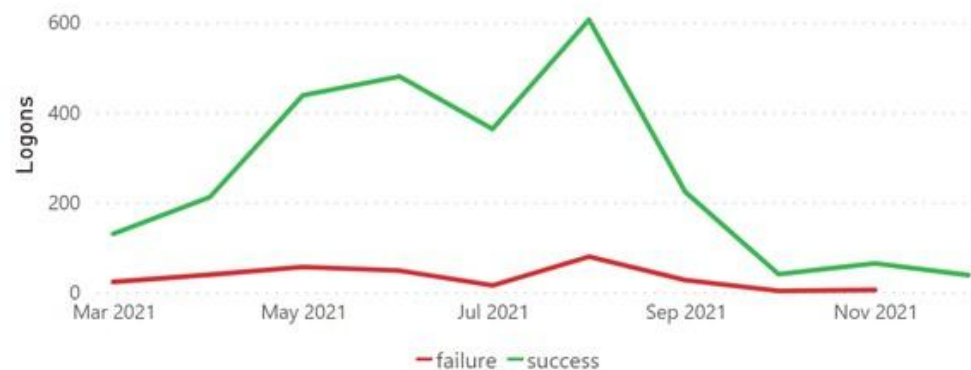
SharePoint

- 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



Windows Logon Audit

Logon Outcome over Time



Date Range

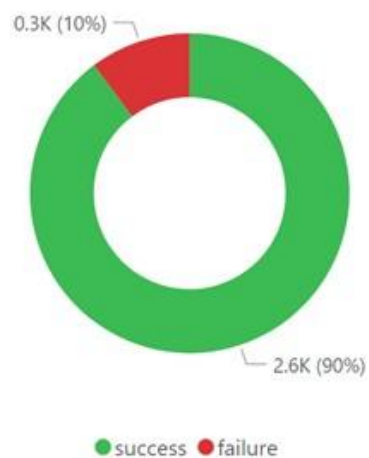
3/22/2021



12/31/2021



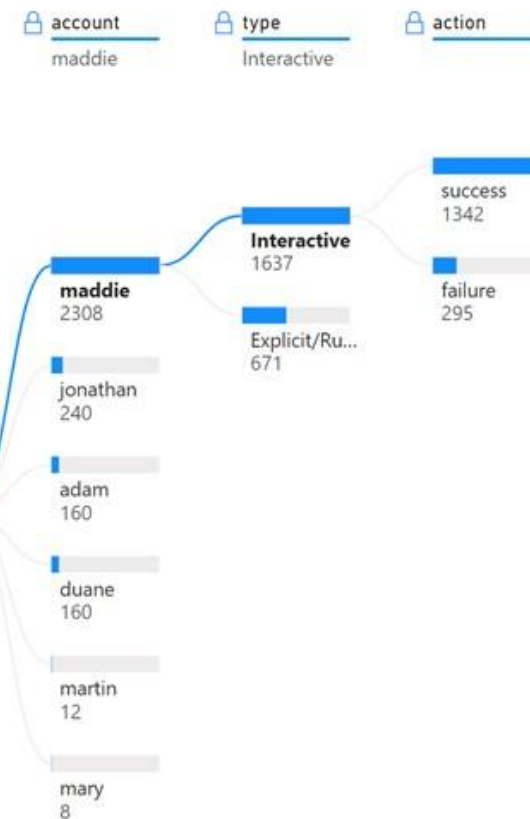
Logon by Outcome



Logon Outcome by Type

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

Logon Details by User



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

