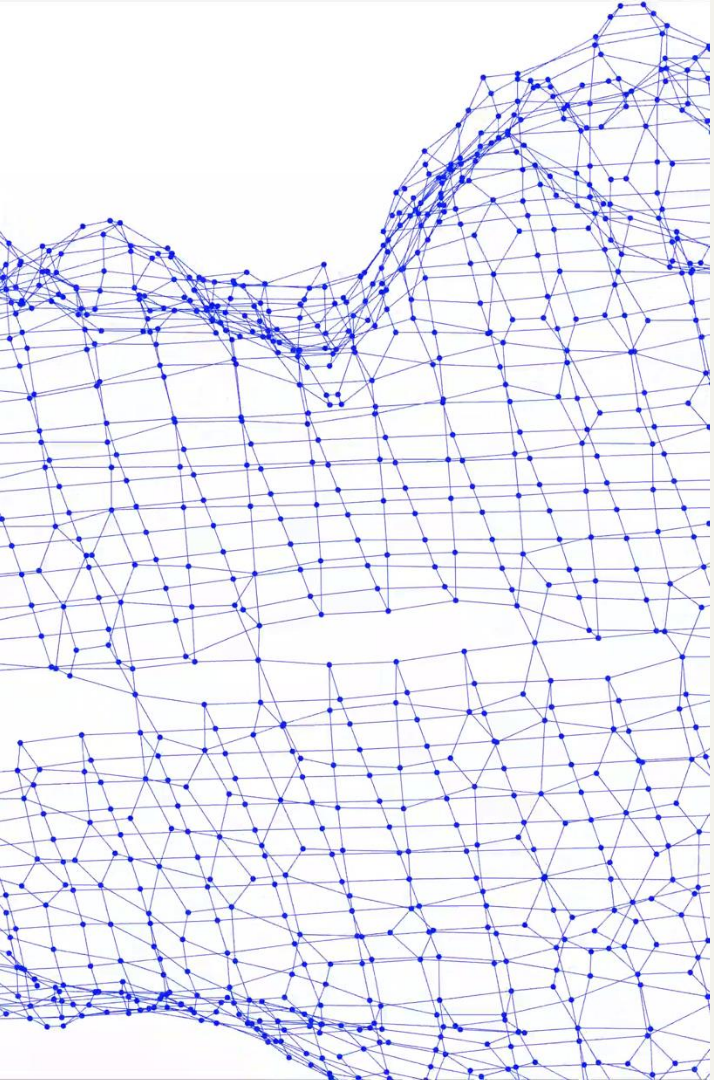


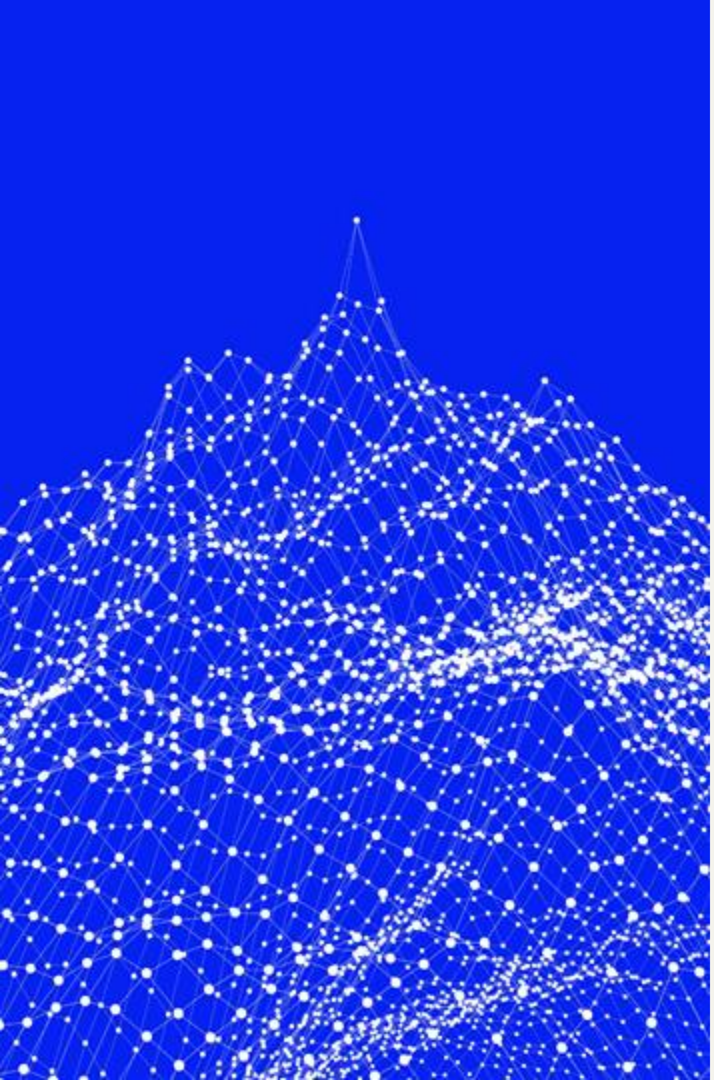
FME Flow: Secure and Clean

Abley

Todd Davis

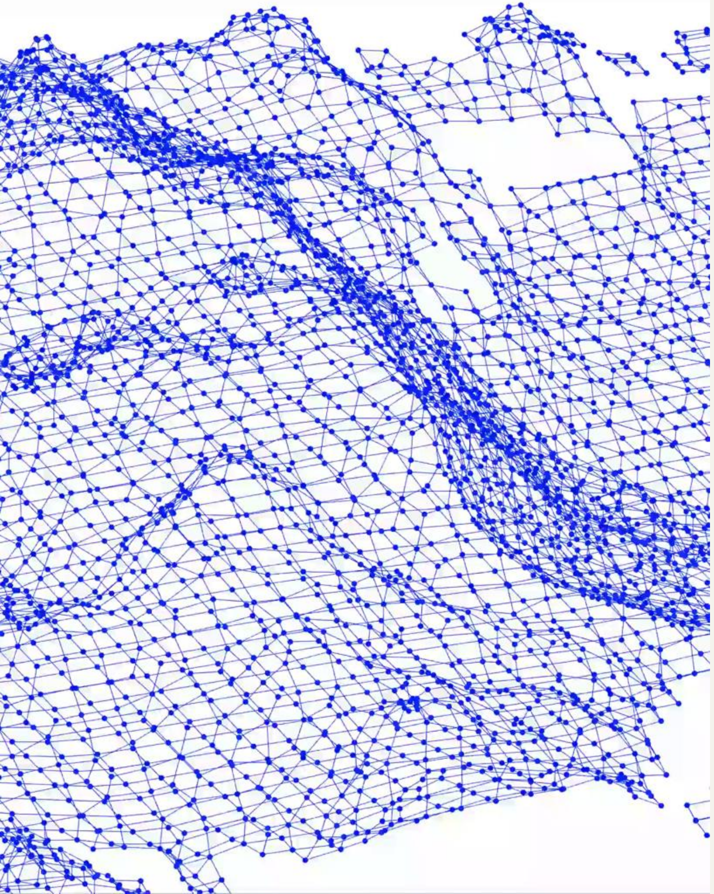
Technical Director

ably



Agenda

1. Introduction
2. Why it matters
3. What occurs
4. Outcome
5. Conclusion



Section 1

Introduction

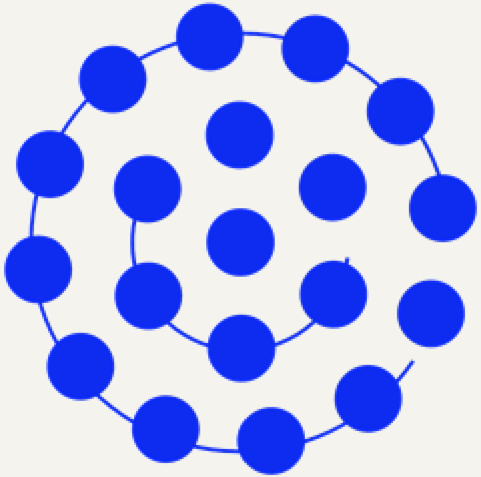
Risk Perception is people's subjective judgement about the likelihood of negative occurance.

You care about risk, when you understand it!

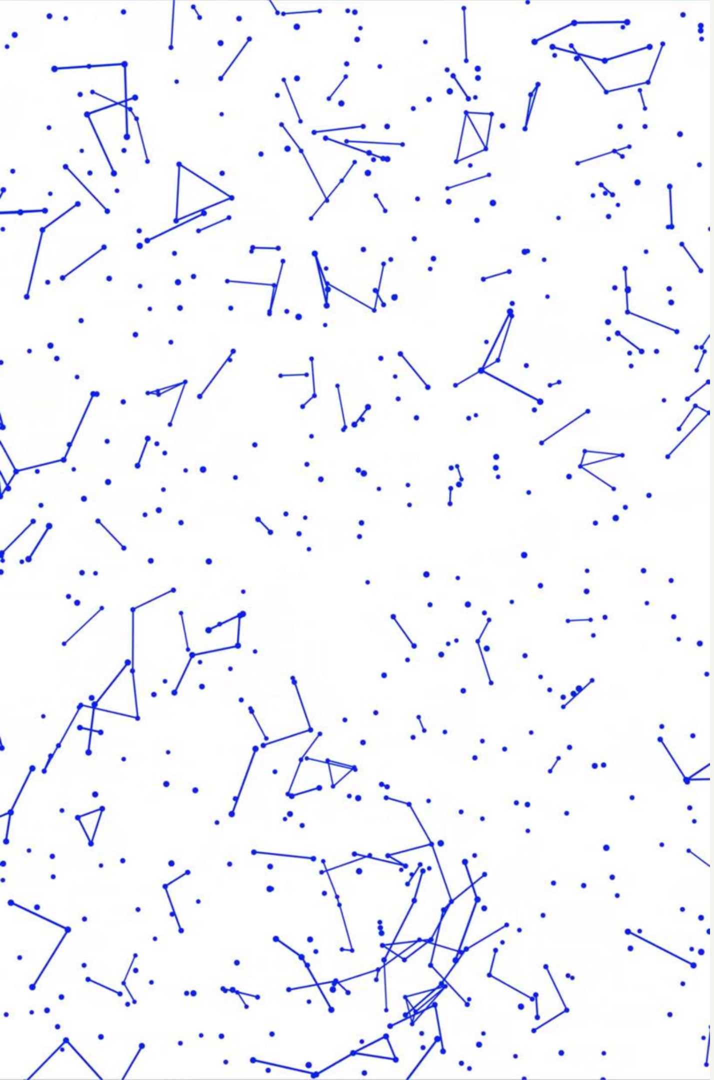
By keeping FME Flow secure and clean, you reduce the chances of having a negative occurance.

You can also have greater confidence that things are working correctly and threats are reduced.

In many cases that means your users have good experiences.



At Abley, we have developed comprehensive processes to support our client’s FME Flow environment.

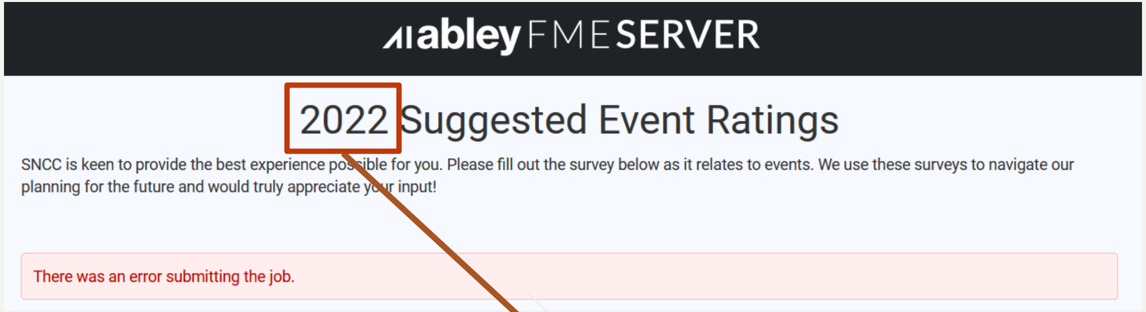


Section 2

Why it matters?

Nobody wants to see a failure.

- Disrupts progress
- Creates pressure
- Reduce confidence



2022 Suggested Event Ratings

SNCC is keen to provide the best experience possible for you. Please fill out the survey below as it relates to events. We use these surveys to navigate our planning for the future and would truly appreciate your input!

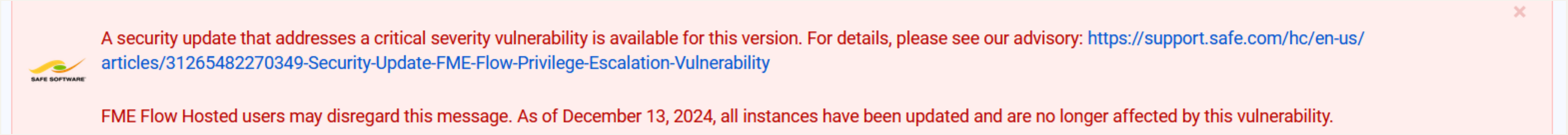
There was an error submitting the job.

- We won’t stop all failures, but less is aways better.
- We also need to learn from failure.

And how about making sure things are still relevant!

And then there is security.

Software companies do great work fixing vulnerabilities



A security update that addresses a critical severity vulnerability is available for this version. For details, please see our advisory: https://support.safe.com/hc/en-us/articles/31265482270349-Security-Update-FME-Flow-Privilege-Escalation-Vulnerability

FME Flow Hosted users may disregard this message. As of December 13, 2024, all instances have been updated and are no longer affected by this vulnerability.

And when a software company tell your organization there is a patch:

- IT security teams jump.
- Immediate concern about what it means.
- Usually quick to plan an implementation.

- The issue above was around privilege escalation. But...

You don’t need to escalate permissions, if you are given them!

This is not a fault of the software, but a mistake by the person creating the process.

Our experience show that most environment have these accidents occur.

Even the most diligent operators can leave a door open.

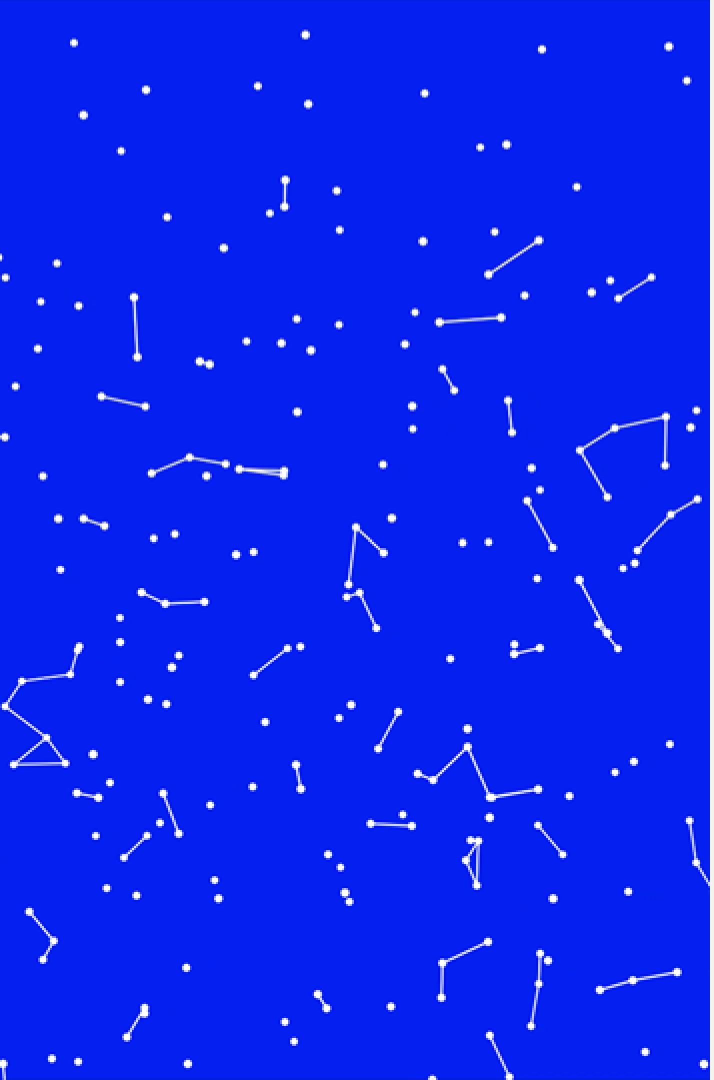
So automating checks provide reassurance.

To prove a point…

I randomly found 3 public endpoint and used standard api calls to see how relevant this could be in the wild.

- From 1st URL: Found 11 Server apps, and got access to run 19 workspaces.
- From 2nd URL: Found 1 Server app and couldn't do anything more than run it. (Congratulations!)
- From 3rd URL: Found 3 Server apps, was able to run 73 workspaces with 3 associated connections.

Could they be processes that would give me information, or allow me to alter internal data?



Section 2

What occurs?

Getting all aspect of FME Flow

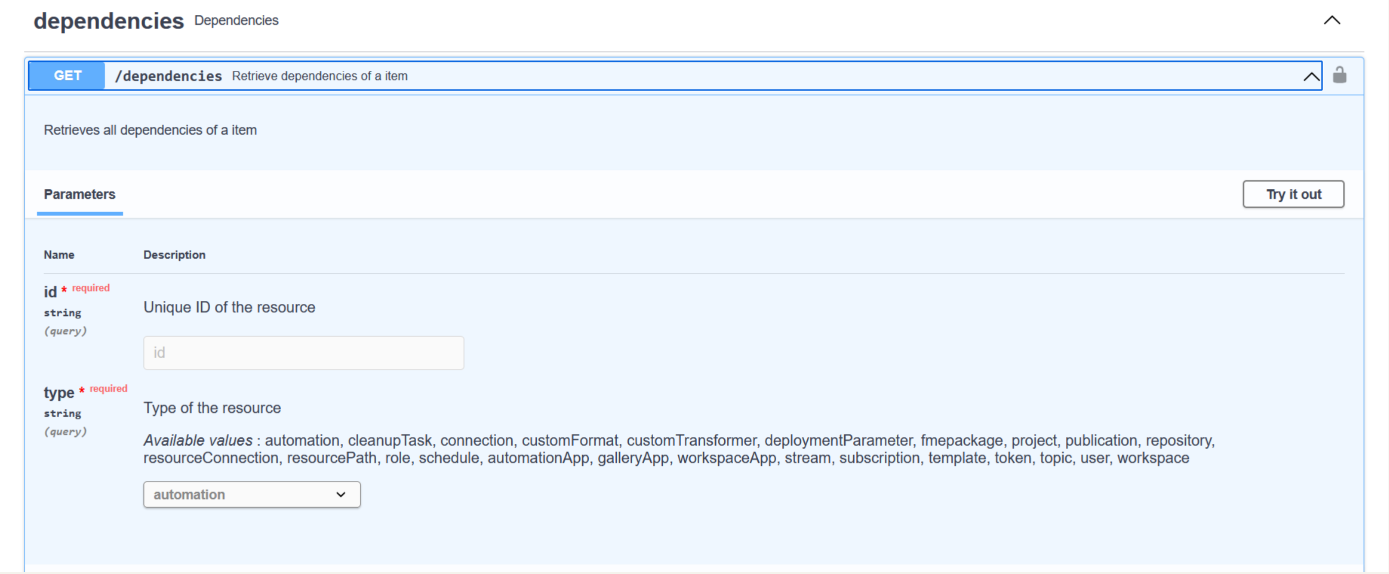
Initial process to get the data:

- FME Rest API provides data about FME Flow.
- Extract all aspect of workspaces on FME Flow.
- Always updating for new endpoints.
- Once you have all the data, you can look at any scenario.

There are so many options in FME Flow to achieve a desired result.

Safe is also expanding inbuilt ability

- V4 of FME Flow Rest Api for dependencies



dependencies Dependencies

GET **/dependencies** Retrieve dependencies of a item

Retrieves all dependencies of a item

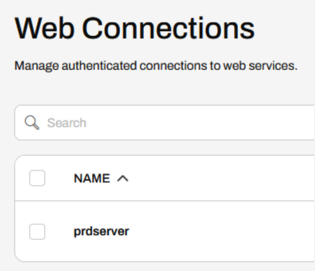
Parameters

Try it out

Name	Description
id * required string *(query)*	Unique ID of the resource id
type * required string *(query)*	Type of the resource *Available values* : automation, cleanupTask, connection, customFormat, customTransformer, deploymentParameter, fmepackage, project, publication, repository, resourceConnection, resourcePath, role, schedule, automationApp, galleryApp, workspaceApp, stream, subscription, template, token, topic, user, workspace automation

Lets look at example of relationships in FME Flow

- “Big Company” used a “prdserver” connection for accessing ArcGIS Enterprise.
- FME and ArcGIS are growing, and the connection uses an admin user to connect. It has too many permissions.
- They need to switch to the new “datareader” user, by using a new “prdserver...datareader” and a “prdserver...adminuser” connection for ArcGIS admin functionality.

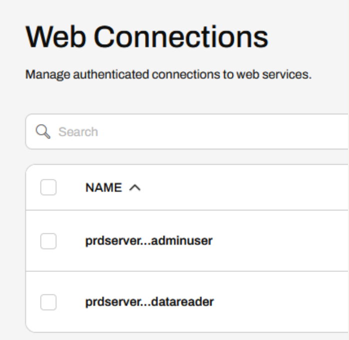


Web Connections

Manage authenticated connections to web services.

□	NAME ^
□	prdserver

So they deleted the “prdserver” connection and replaced it with two new connections



Web Connections

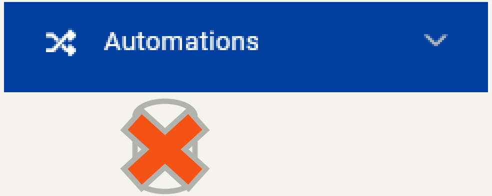
Manage authenticated connections to web services.

□	NAME ^
□	prdserver...adminuser
□	prdserver...datareader

Finding the relationship

In just one automation app the “prdserver” connection is used multiple times :

- It is included as a parameter in one of the workspaces, and is selected in the automation.
- Inside another workspace, but it that case, not parameterized.
- Is listed in the token that is associated with the automation app.



Now lets look at security

Once we have all the information about an FME Flow, here is an example of what we can look for:

Accidental Workspace release

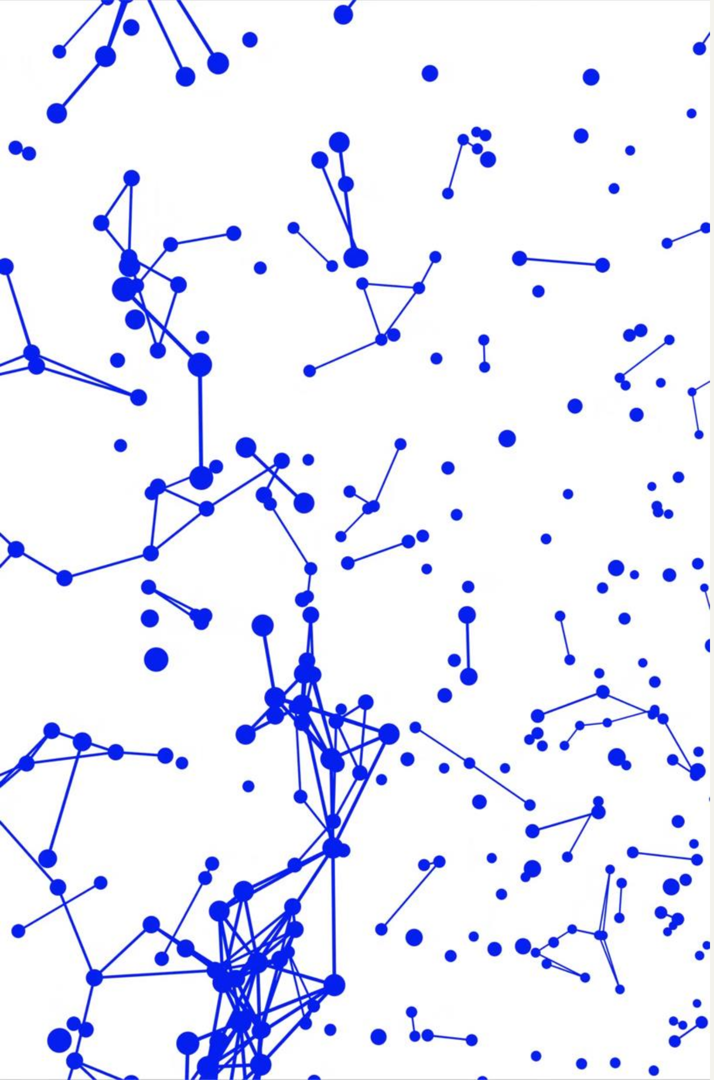
Excessive Token Permissions

Public access to private data

Username/Password in workspace

Processes that could give access to wider realm

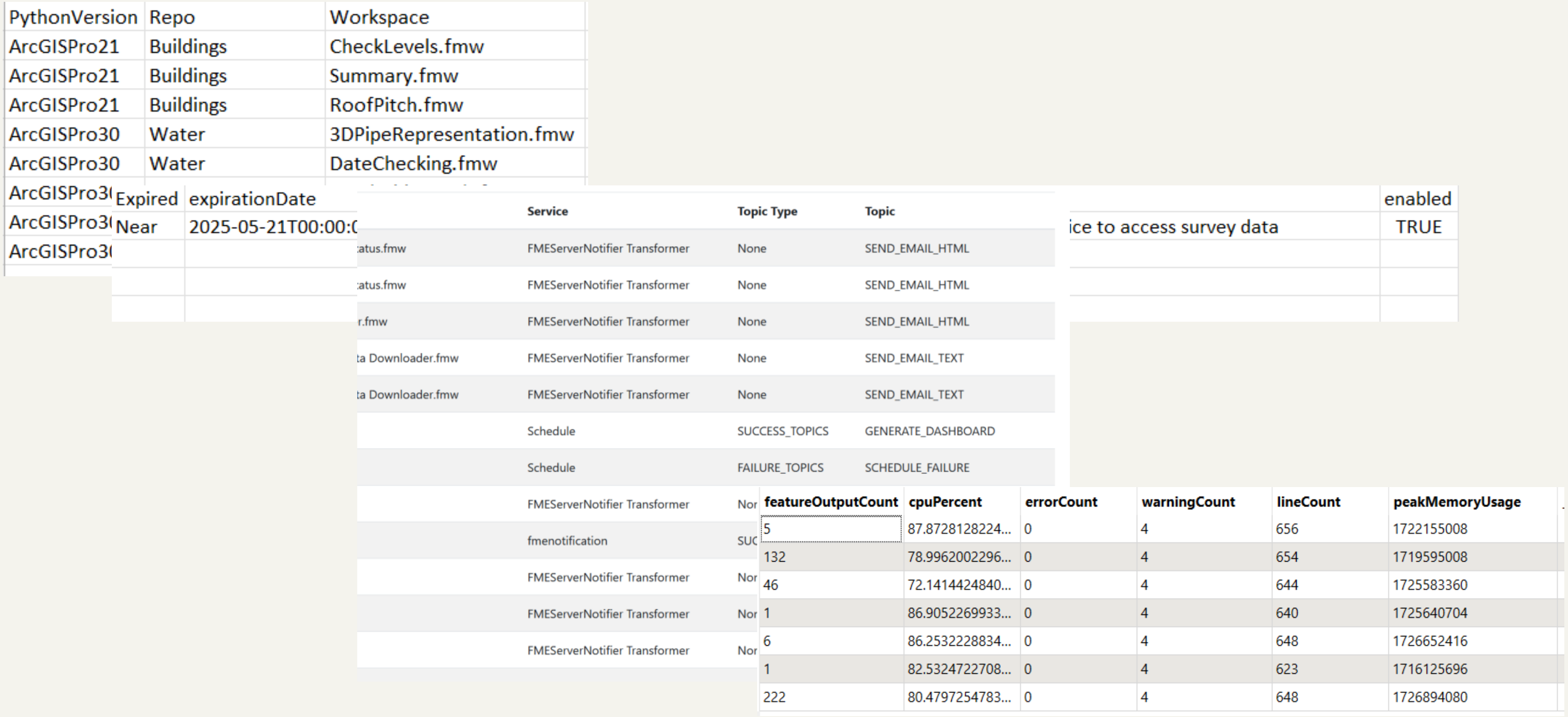
SQL Injection



Section 4

Outcomes

It’s not a pretty map, but it’s important data



PythonVersion	Repo	Workspace
ArcGISPro21	Buildings	CheckLevels.fmw
ArcGISPro21	Buildings	Summary.fmw
ArcGISPro21	Buildings	RoofPitch.fmw
ArcGISPro30	Water	3DPipeRepresentation.fmw
ArcGISPro30	Water	DateChecking.fmw
ArcGISPro3(		
ArcGISPro3(		
ArcGISPro3(		

Expired	expirationDate
Near	2025-05-21T00:00:(

	enabled
ice to access survey data	TRUE

	Service	Topic Type	Topic
:atus.fmw	FMEServerNotifier Transformer	None	SEND_EMAIL_HTML
:atus.fmw	FMEServerNotifier Transformer	None	SEND_EMAIL_HTML
r.fmw	FMEServerNotifier Transformer	None	SEND_EMAIL_HTML
ta Downloader.fmw	FMEServerNotifier Transformer	None	SEND_EMAIL_TEXT
ta Downloader.fmw	FMEServerNotifier Transformer	None	SEND_EMAIL_TEXT
	Schedule	SUCCESS_TOPICS	GENERATE_DASHBOARD
	Schedule	FAILURE_TOPICS	SCHEDULE_FAILURE
	FMEServerNotifier Transformer	Nor	
	fmenotification	SUC	
	FMEServerNotifier Transformer	Nor	
	FMEServerNotifier Transformer	Nor	
	FMEServerNotifier Transformer	Nor	

featureOutputCount	cpuPercent	errorCount	warningCount	lineCount	peakMemoryUsage
5	87.8728128224...	0	4	656	1722155008
132	78.9962002296...	0	4	654	1719595008
46	72.1414424840...	0	4	644	1725583360
1	86.9052269933...	0	4	640	1725640704
6	86.2532228834...	0	4	648	1726652416
1	82.5324722708...	0	4	623	1716125696
222	80.4797254783...	0	4	648	1726894080

Proactive

- The token on that workspace app is due to expire in two months.
- The workspace associated with the server app has been deleted.
- The automation has been disabled for several months.
- The process has been updated, but hasn’t been commited to Git.
- We are seeing large queing of jobs at this time, due to multiple schedules.

Reactive

From Client’s:

- Can you tell me all the processes that send an email to...
- The url to their ArcGIS Enterprise server, can you find all the locations where that is defined.
- Can you tell me all the repositories, schedules, automations that use this queue.

From Us:

- The Server App has been given permission to read/write to the Data resources folder. Does it need that permission?
- The Server App utilises a workspace in a repo with many other processes. The token has permission to also run those other workspaces.

Section 5

Conclusion

Spend more time doing the things you enjoy!

Not dealing with problem when they arise.

Constant improvement

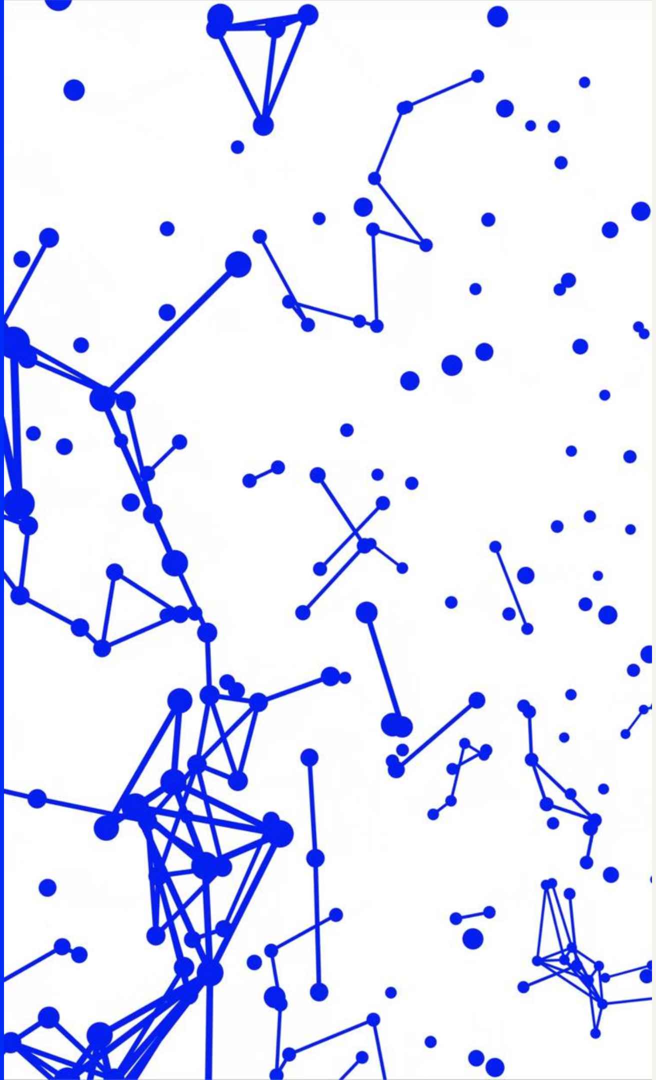
People want to do a good job and our processes help that:

- Help shut the door on intrusion
- Raise the awareness of risk
- Reduce the chances of negative occurence

But the biggest improvement... We grow the knowledge of the staff we work with.
Growth is accelerated.

Shining a light onto it!

Question: Is there demand for this capability?



Come see me:

If you want to see what the data looks like, and all the things that get extracted.

Plus, if you have public server apps and are keen to see if you have got any issues visible.

Thank You

Todd Davis
Abley
todd@abley.com