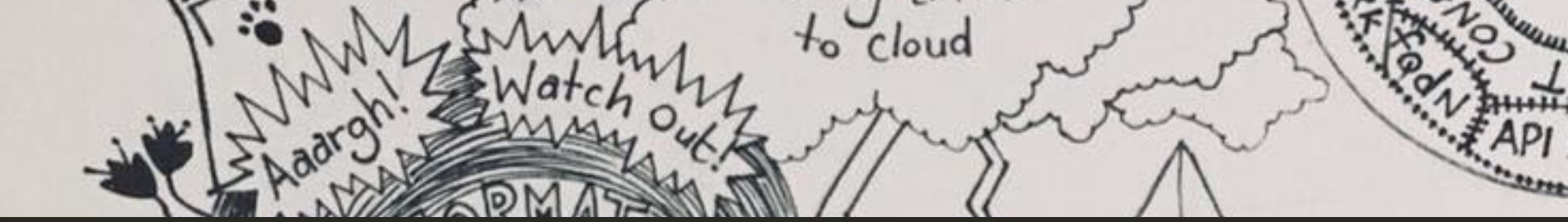


DEVSECOPS FIELD NOTES

FinTech Field Notes
from a Technical Director

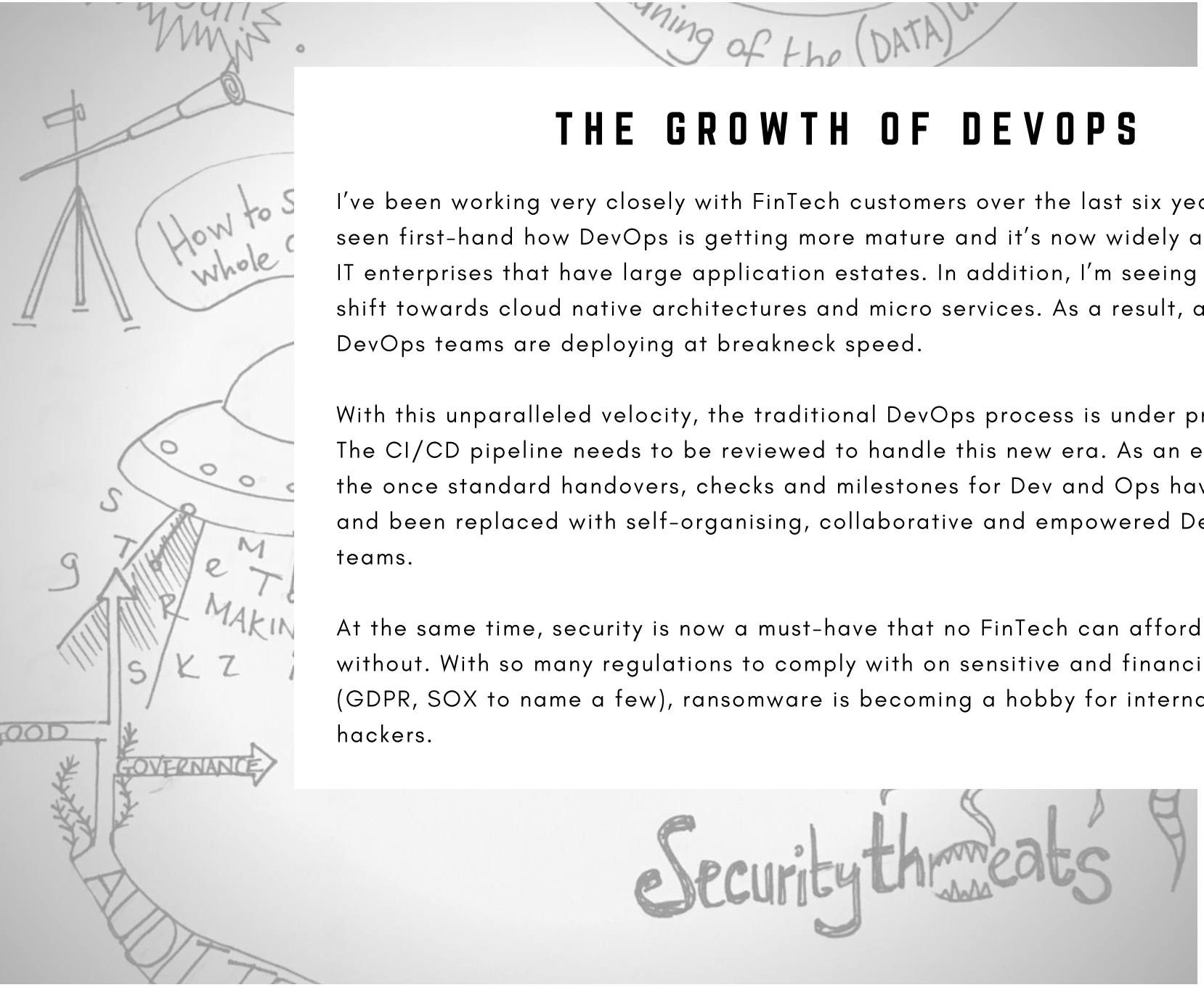
Author: Ben Riley
www.sweagle.com

THE MEANING OF DEVSECOPS AND HOW TO AVOID DATA BLACK HOLES

If you're reading this, it's pretty safe to assume that you know DevOps is no longer just a fluffy concept. It's now the standard for agile projects and deliveries. Today, information is actively shared between Dev and Ops, with multiple teams delivering more features and a plethora of changes going through production faster than ever before.

But why has a security component crept into DevOps? Why the new buzzword and what was wrong with plain old DevOps? Where did this new-fangled term come from and do we need to bother with it?

Author: Ben Riley
www.sweagle.com



THE GROWTH OF DEVOPS

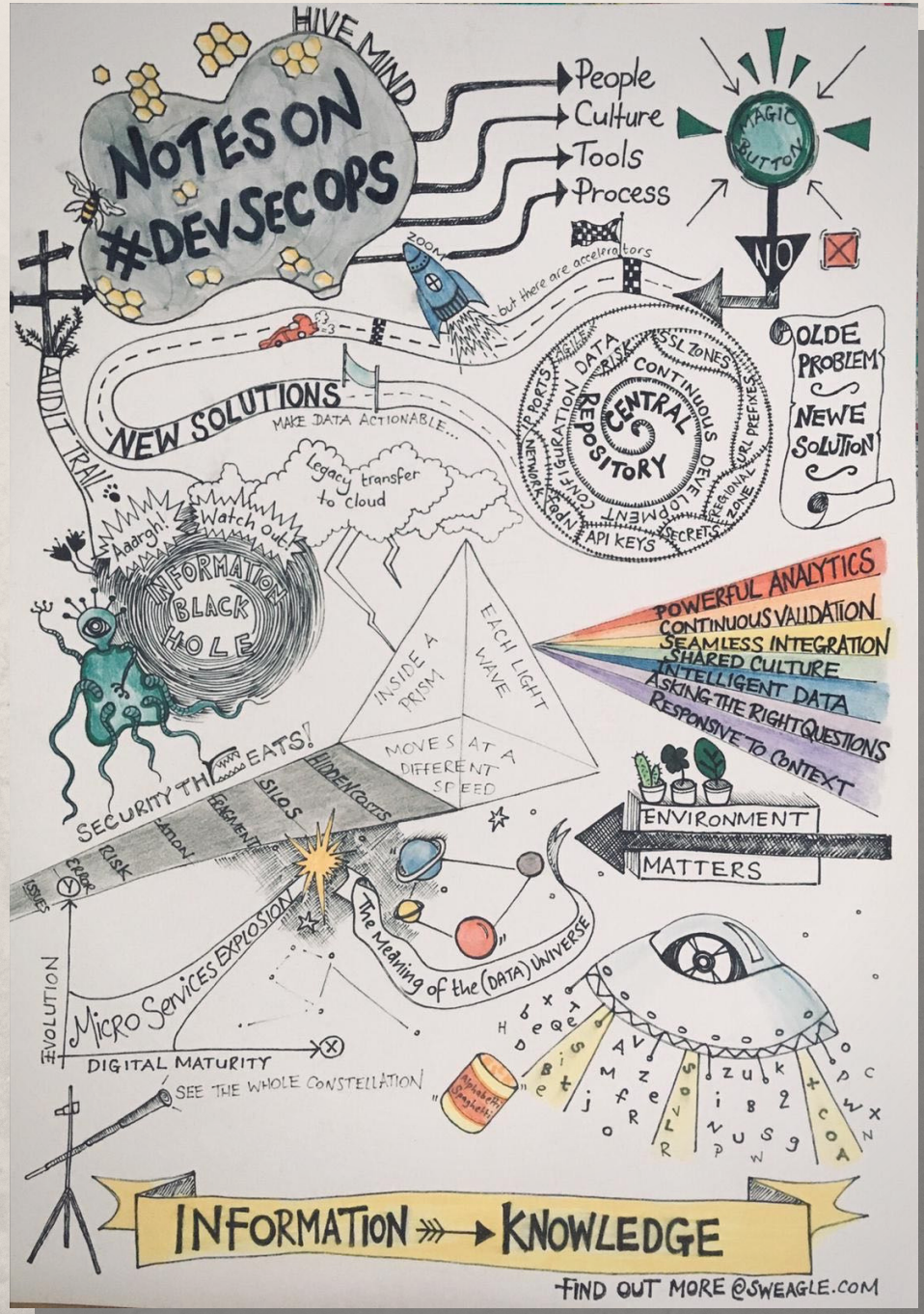
I've been working very closely with FinTech customers over the last six years. I've seen first-hand how DevOps is getting more mature and it's now widely adopted in IT enterprises that have large application estates. In addition, I'm seeing a rapid shift towards cloud native architectures and micro services. As a result, agile DevOps teams are deploying at breakneck speed.

With this unparalleled velocity, the traditional DevOps process is under pressure. The CI/CD pipeline needs to be reviewed to handle this new era. As an example, the once standard handovers, checks and milestones for Dev and Ops have vanished and been replaced with self-organising, collaborative and empowered DevOps teams.

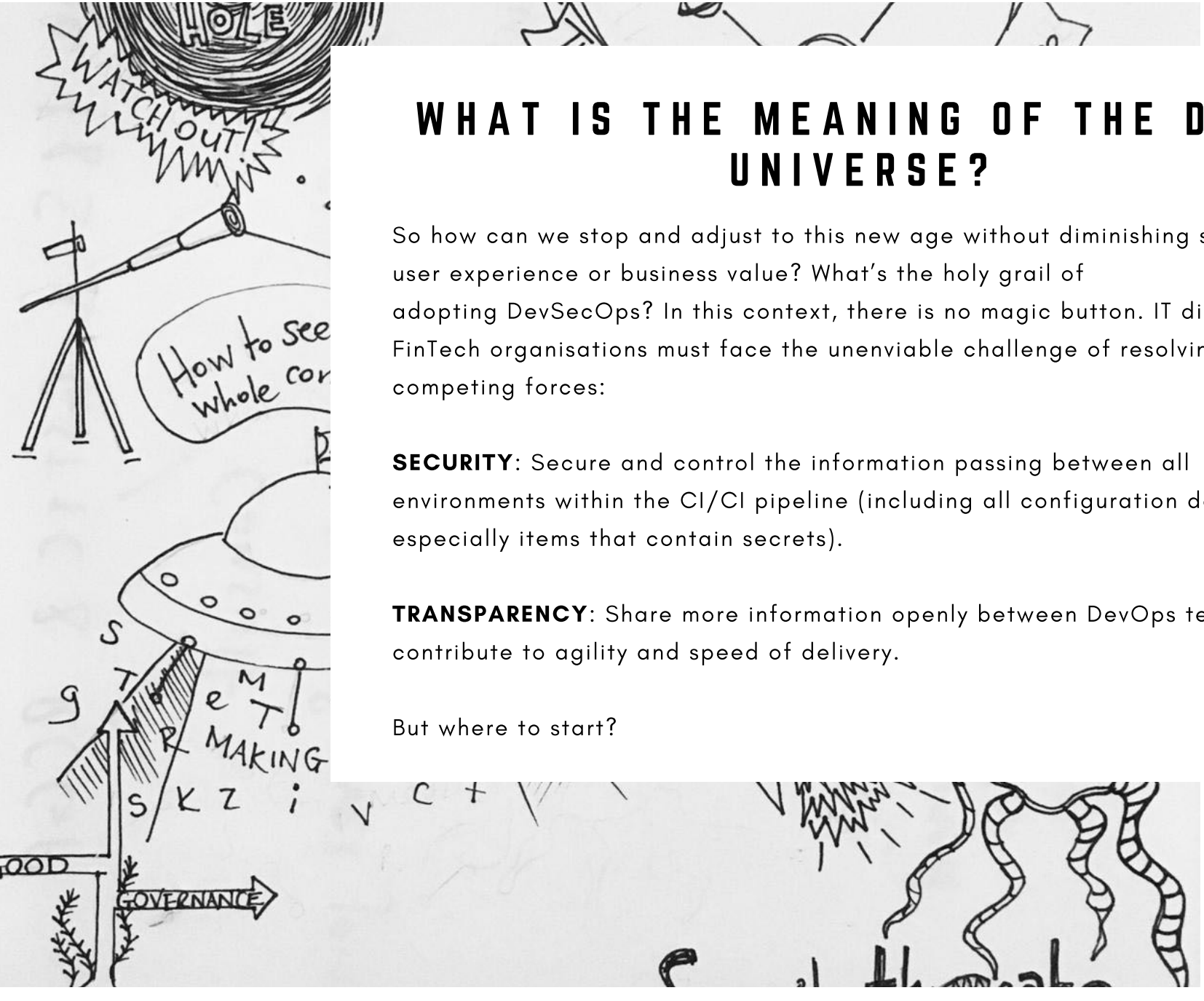
At the same time, security is now a must-have that no FinTech can afford to be without. With so many regulations to comply with on sensitive and financial data (GDPR, SOX to name a few), ransomware is becoming a hobby for international hackers.

THE CURRENT UNIVERSE

The current universe of DevSecOps in FinTech today is a cacophony of command and control, with validation and security wielding its merry way through realms of disconnected audit trails. What's more, this spider's web of hoops and loops simply cannot cloak the creativity, value or quality of application deployment in competitive FinTechs. DevOps teams should feel confident that they can do their job without breaking compliance rules and the tools they use should protect them from any regulatory breaches.



CLICK TO ENLARGE



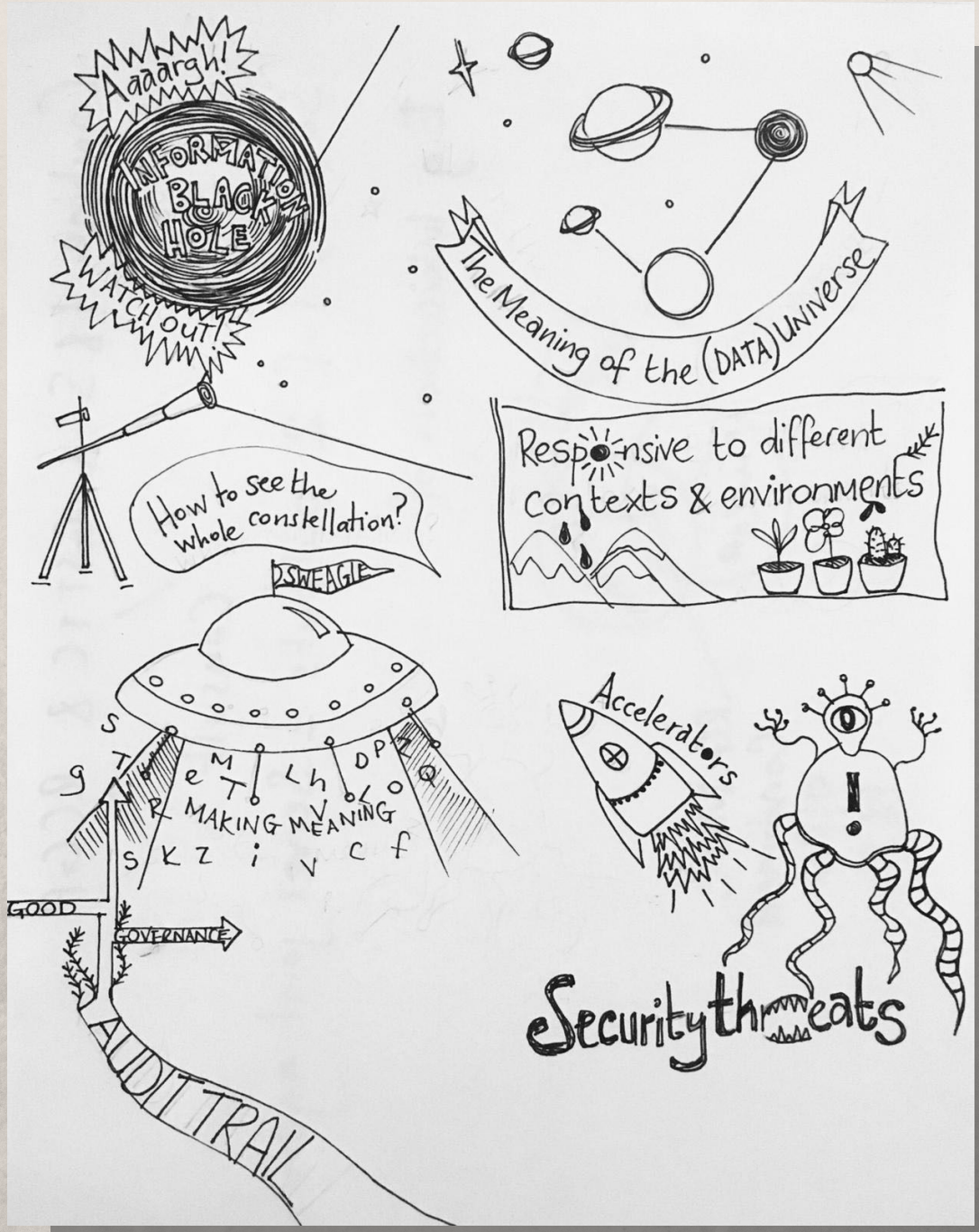
WHAT IS THE MEANING OF THE DATA UNIVERSE?

So how can we stop and adjust to this new age without diminishing speed, user experience or business value? What's the holy grail of adopting DevSecOps? In this context, there is no magic button. IT directors of FinTech organisations must face the unenviable challenge of resolving two competing forces:

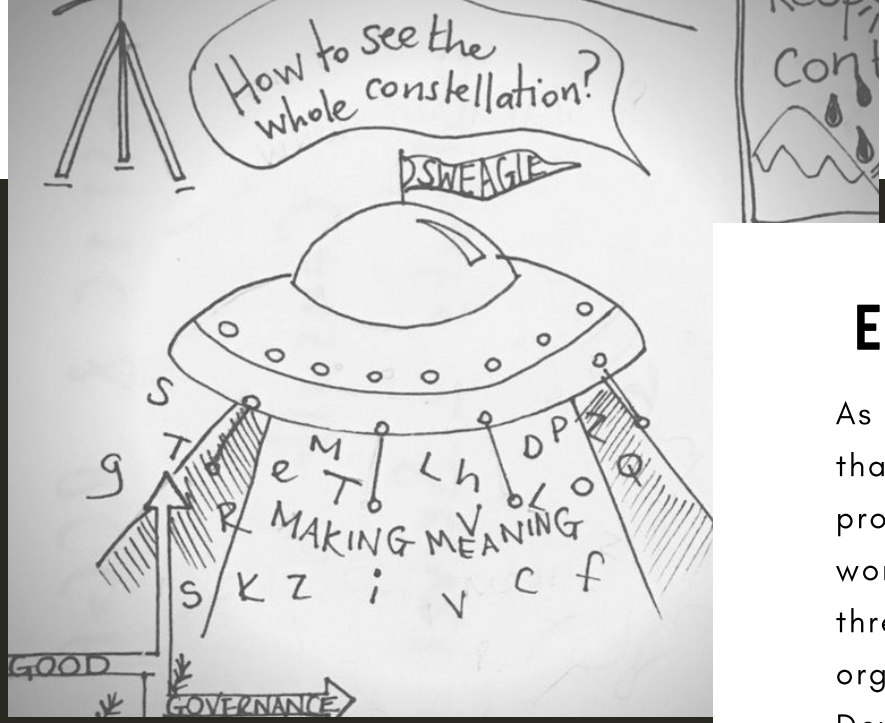
SECURITY: Secure and control the information passing between all environments within the CI/CI pipeline (including all configuration data, especially items that contain secrets).

TRANSPARENCY: Share more information openly between DevOps teams to contribute to agility and speed of delivery.

But where to start?



CLICK TO ENLARGE



ENVIRONMENT MATTERS

As a regulated industry, FinTechs are well aware that malicious changes can make it into their production environments by accident – or even worse – on purpose. Let's face it, one of the major threats for FinTech today comes from inside the organisation. At the end of the day, with your DevOps teams on steroids (so to speak), your process is open to new vulnerabilities and new types of security threats.

And, inside the application prism, the Environment really does matter. Can you prove to the auditors and regulators that you have full command of your data universe and know exactly how every application was running, at any given moment in time, in every environment?

What did it look like before and after every change? Where did the change come from? Who applied it? And in a regulated industry, you need to have all the answers at your fingertips. This is why those three little letters in the middle of DevSecOps are so explosive right now.

Watch out for the black hole!

How do you avoid the data black hole? From spending time with FinTech customers over the last 6 months, I've boiled it down to five stages.

You can implement these steps today to see an immediate improvement in quality and speed...

5 STEPS TO AVOIDING DATA BLACK HOLES

Step 1: Collect all configuration data, across all environments, in a central “agnostic” repository. If it’s all in one place, not only you control it but you build a complete “evidence repository” to support your quality control and governance processes.

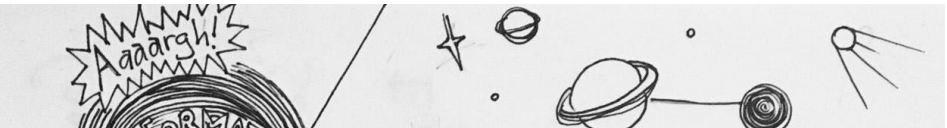
Step 2: open API, but with strong permissions control for both people and systems. Share and distribute information with role based access control RBAC.

Step 3: Secure and encrypt all sensitive data. Without exception. Secrets should never make it in plain text into production and if they do, locate that source and correct the process so it can never happen again.

Step 4: Seamlessly integrate continuous validation into the DevOps pipeline without impacting speed and agility. Easier said than done but it is possible. It’s like an insurance policy. If you take out the policy now, you are securing the future of your application estate, in perpetuity.

Step 5: Track and detect any changes with a robust audit trail that allows root cause analysis and diffComparison - be ready to understand within seconds what has changed for a given application in a given environment between “now” and “18 hours ago” - from application, environment and infrastructure point of view.

And, in very simple terms, that’s it. One small step for FinTech, one giant leap for DevSecOps.

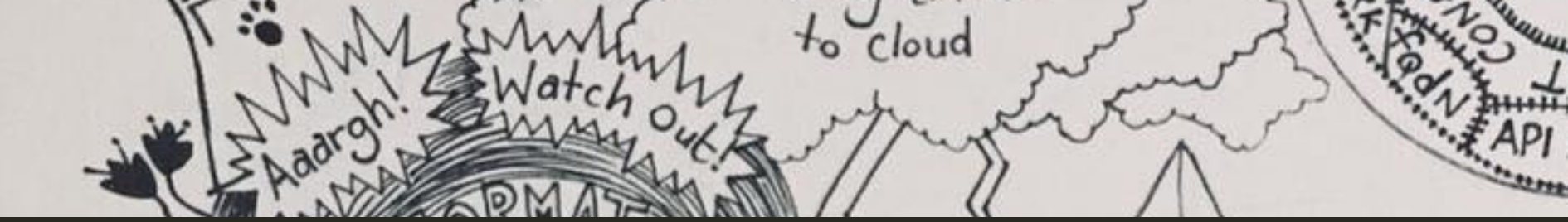


THE FUTURE OF DEVOPS

So, what does the future hold for DevOps? In my opinion, by 2025, all FinTech organisations will deliver through automated pipelines. We will all accelerate deliveries further with new DevSecOps practises. And everyone will be more data driven.

By 2025, if you're unable to prevent things from going off track and catch anomalies before they are applied, then you're aboard a sinking ship. Even when our DevOps teams are working with a high level of automation, you will need to have a proactive configuration data management platform to keep a constant eye on all these high speed changes. In 2025, your CI/CD pipeline will be proactively managed by an intelligent, automated and machine-learning force that will continuously validate deployments 24/7. It won't matter if the changes being applied are technical, functional or sensitive, because it will all be handled by a multi-faceted platform which has learnt everything about your pipeline through past activity.

So, you can actually predict the future. In doing so, you can also protect your application estate from colliding with any external or internal threats.



THE AUTHOR

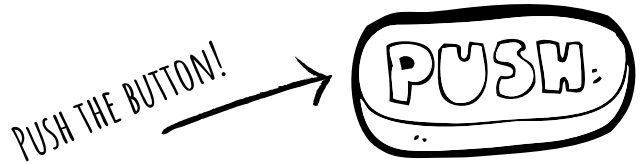
Ben Riley is Technical Director at Sweagle. He helps FinTech customers to embrace the speed of DevOps changes while maintaining security and control of their most important technical assets: their configuration data.

FinTech Field Notes
from a Technical Director

UP NEXT...

Register for our upcoming FinTech webinar streaming live on September 17 2019 and on catch up afterwards:

How to make DevSecOps and CI/CD automation a winning combination in regulated industries



Author: Ben Riley
www.sweagle.com