# WHO ARE WE

Pulak Agrawal
*DevSecOps Practice Lead, Accenture UK*

Fortune Barnard
*Director of Digital Security and Resilience, Virgin Media O2, UK*

Karel Kohout
*Managing Director, Accenture Europe Application Security Lead, Czech Republic*

# VIRGIN MEDIA 2021 – COMPANY BACKGROUND

## 2nd largest broadband provider in the UK

Virgin Media is a British telecommunications company which provides telephone, television and internet services in the United Kingdom. Its headquarters are at Green Park in Reading, England.It is owned by VMED O2 UK Limited, a 50:50 joint venture between Liberty Global and Telefónica.

Virgin Media owns and operates its own fibre-optic cable network in the United Kingdom, although optical fibre does not reach customer premises, instead going to a nearby street cabinet to provide a fibre to the cabinet service. As of 31 December 2012, it had a total of approximately 4.8 million cable customers

# VIRGIN MEDIA AND O2 JV

**Two of the biggest players in telecom were going to be entering a JV**

On 7 May 2020, Liberty Global reached an agreement with Telefónica to merge their UK businesses, Virgin Media and O2, in a deal worth £31bn. The Competition and Markets Authority approved the merger in May 2021, and the merger was to be completed on 1 June 2021 (**6+1 weeks before we started this project**).This created one of the UK's largest entertainment and telecommunications companies. The resulting company is called VMED O2 UK Limited.

Apart from the size of the merger, part of the IT systems integration needed to be very quick, for shareholder value and end consumer benefits.


We knew Conway’s Law will influence us

*Any organization that designs a system will produce a design whose structure is a copy of the organization's communication structure – Melvin Conway*

# PROBLEMS

**The security approvals were REALLY slow, and would have impacted business**

VM have security approval processes at each stage of lifecycle from design to production. These processes inadvertently translated into very busy security teams and long wait times for approvals (6-8 weeks) which were exacerbated as VM follows a strict zero-trust security model.

- Siloed manual security governance process which meant redundant security testing
- Limited security team bandwidth meant weeks of wait before anything could be approved
- The ever-increasing number of security threats (increased manifold during the pandemic)
- The need for digitisation meant newer technology investments and evolving security postures, security fatigue and toil.
- Limited visibility of vulnerabilities leading to business risks and exposure
- The Digital business were building next gen microservice platforms, requiring delivery pace and new ways of working

# WHAT COULD WE DO ?

**C level sponsorship; speed without compromise on security; implement modern DevSecOps principles**

To address the problems, the Chief Digital Officer commissioned a DevSecOps project for left shifting security to accelerate delivery and flow and start changing the culture and a team was created with direct reporting into the C suite

The required characteristics of the system

- Left-Shifted Security
- Security by Design
- Privacy by Design
- Self Serve
- Single View of Vulnerabilities
- Everything-as-code

# APPROACH TO SECURITY TESTING

## All round security

| BASELINE SECURITY | CONTINIUOUS, INTEGRATED SECURITY (SDLC) | SECURE CLOUD MIGRATION | REMEDIATION |
|---|---|---|---|
| Minimum security for on-prem or cloud hosted applications | Integrate security into each phase of SDLC from Design through Development up to Deployment and Production Run | Security for cloud native apps, containers, K8s, IaC | Minimize risks for custom code and packaged solutions |
| **SECURITY TESTING AS A SERVICE** | **DEVSECOPS AS A SERVICE** | **SECURE SOFTWARE DEVELOPMENT** | **CLOUD SECURITY** | **REMEDIATION AND MITIGATION** |
| • Application Security Testing (SAST/DAST/SCA)<br>• Penetration Testing<br>• Analysis (FPA, Triage, Prioritization)<br>• Products Testing | • Security tools integration<br>• IDE security<br>• Source Control<br>• Deployment-Oversight<br>• Security certification<br>• Security Pod Injection<br>• Code signing | • Security requirements<br>• Secure Design \| Threat Modeling<br>• Security Assessment<br>• Secure Deployment<br>• Security certification (Exit criteria)<br>• Data Security<br>• Software Bill of Materials (SBOM) | • Scanning (registry and OS)<br>• Configuration & checks<br>• Block untrusted images<br>• Runtime protection<br>• Containers & Microservices<br>• Orchestration and Kubernetes<br>• Infrastructure as Code Security | • Auto-Remediation<br>• Auto-Mitigation (RASP, WAF)<br>• Compliance & Regulation<br>• Product Remediation |

**PATENTED INNOVATION FOR ACCLERATION**

**DEFECT TRACKING INTEGRATION**

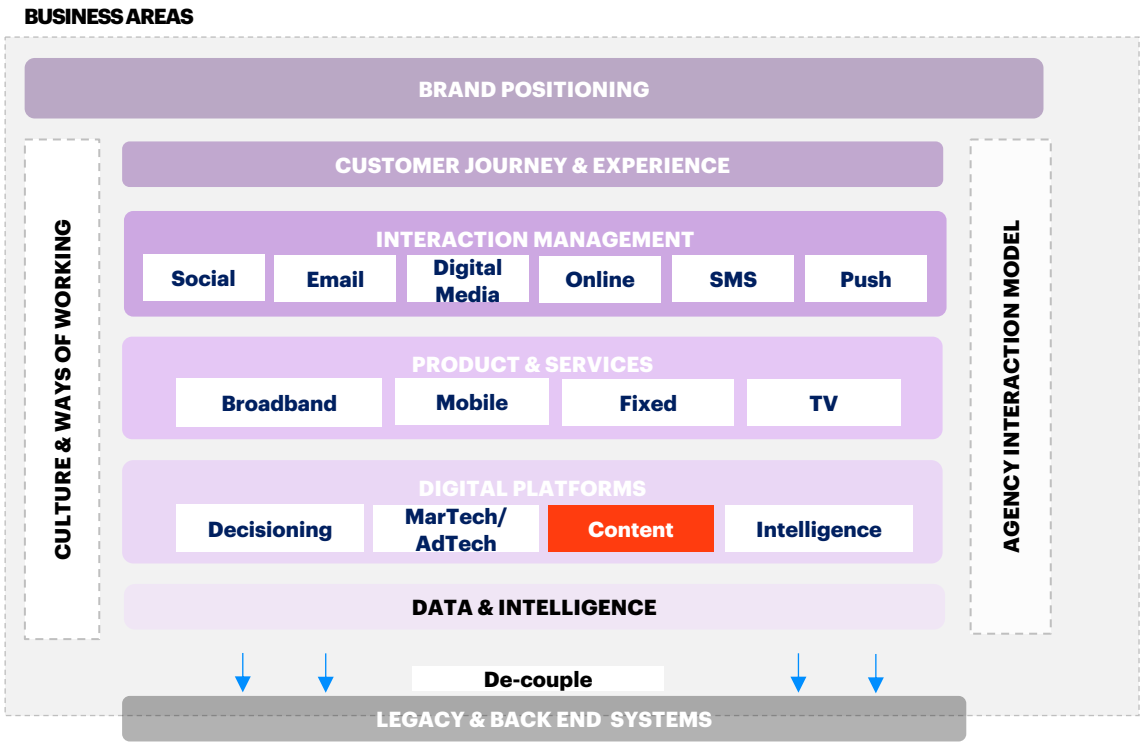
**TRAINING AND CULTURE**

# WORKLOAD SELECTION

**Easy to implement, small, high business value workload; build from scratch on new infra; bring 3rd parties on board**

The project goal was to deliver a content management system application onto a **development** environment built on Google Cloud; utilize tools for SAST, SCA, DAST, container security and threat modelling while providing a single pane of glass.

To power this change, the team were the first consumer of the new container platform (Anthos) and the first live Digital project on VM's new Google Cloud Platform



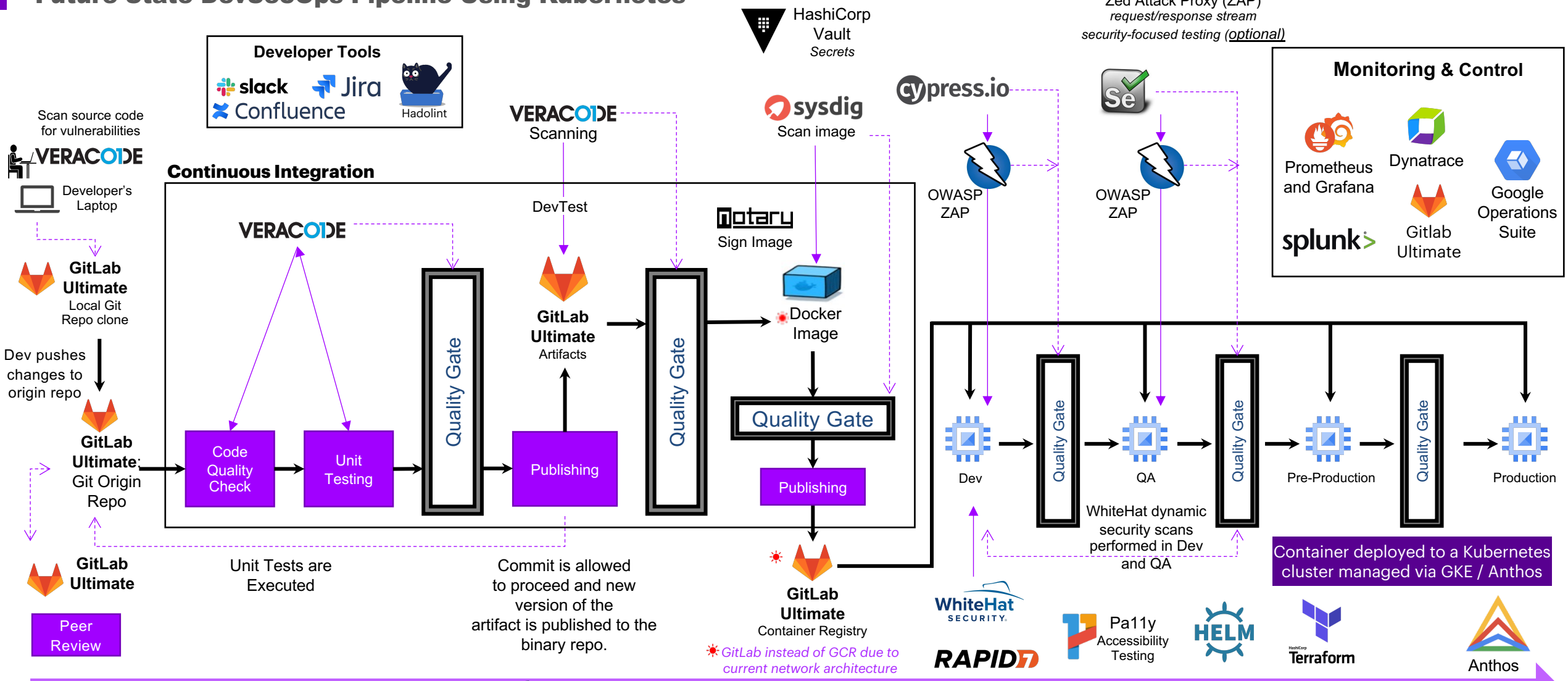

# SELECT THE RIGHT TEAM AND DELIVERY MODEL

**Basics of delivery done right; no compromises on skills; no one is too senior to be disturbed**

- Blended team – badges at the door
- Multi geography team (UK, North America, Czech Republic and India) to ensure the best of the breed DevOps, security SMEs and niche skills (e.g., Google Anthos, Mongo Clustering) were available, while effectively utilizing the follow the Sun model for more hours/day.
- We followed a Kanban approach to deliver this
- Trust your SDLC, your people; your tools ; DRY (Don’t repeat yourself) ; YAGNI (you ain’t gonna need it)
- Pen test in a canary, not in non prod

# SELECT THE RIGHT TOOLS

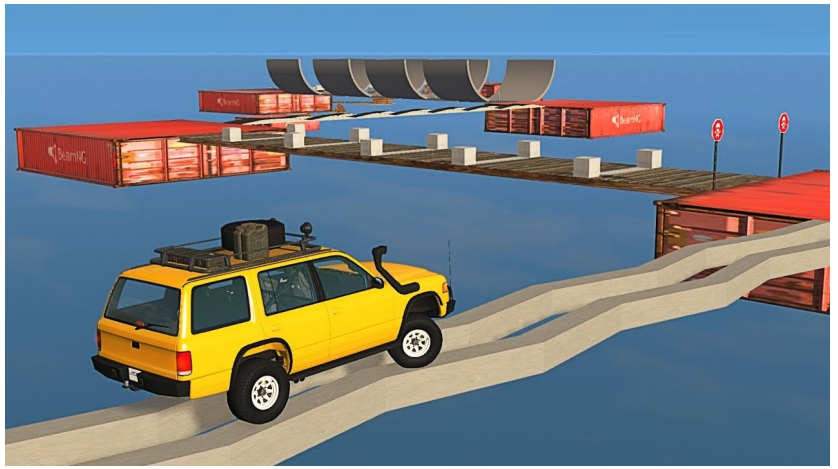
## Future State DevSecOps Pipeline Using Kubernetes



# OBSTACLES TO SUCCESS

**Dirt track racing on a 3-wheeler would probably have been as much fun too**

- Biggest obstacles was the organisational mindset, existing silos and pace of change.
- This was a first project on an evolving container management solution of Google Anthos (GKE on GCP) ; first Application on the new Google Cloud Platform.
- Due to last minute performance requirements, we had to make the systems resilient for 10x the expected volumes by enabling clever caching solutions
- Change in mindset and ways of working change for the security and application teams in a matter of weeks
- Organisational alignment across silo’s and some skills shortages meant initial hesitance in some parts of the organisation
- Security team had to block the go live due to lack of anti-virus solution
- We had to change the DB type based on review from the architecture team, which had limited support from  by the CMS application vendor
- During the supply chain security testing we found a security bug in the CMS product itself and worked with the vendor to help mitigate it for future releases for their other customers



# SHIFTING PRIORITIES

**In the end its about the business and sometimes IT is just an enablement function**

The original scope of this application was an MVP in non-production. Towards the end of the project, because of a successful dev delivery, a decision was made to promote the application to production with 3 days notice (with no production infrastructure in place at the time)

To do this without any additional cost impact we had to trade off nice to have features

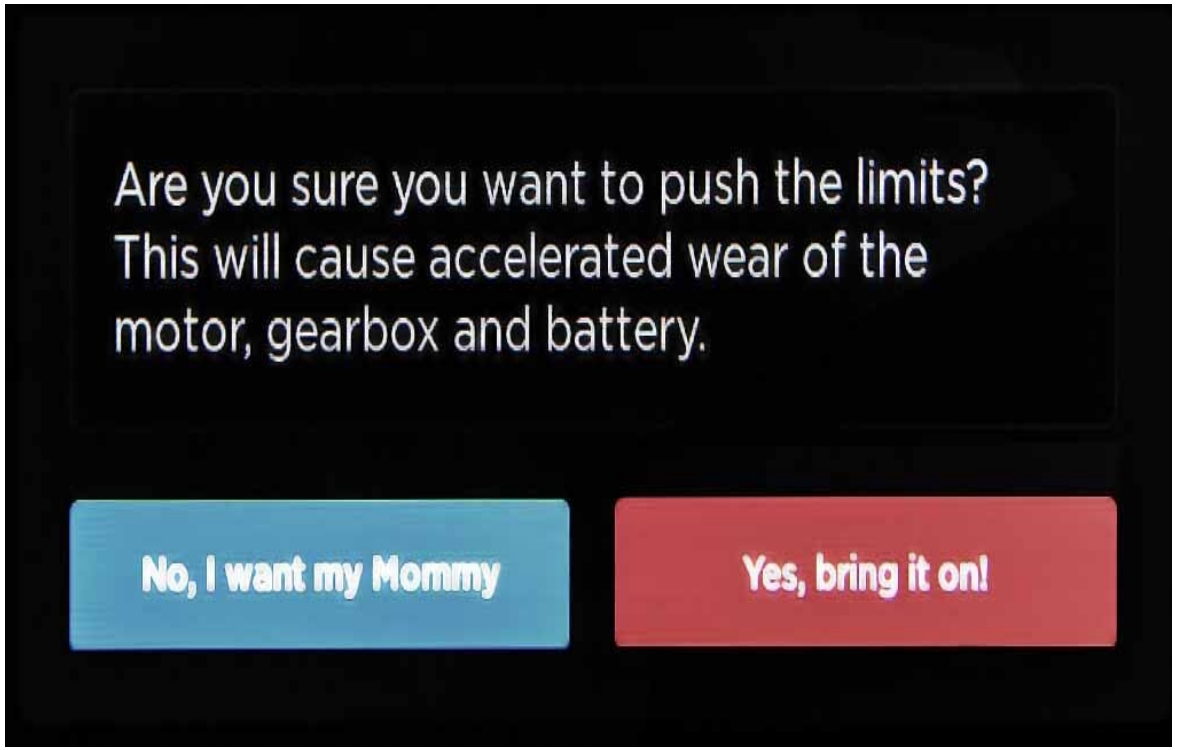
Anti-virus solution deployed to production first in a controlled manner and then retrofitted to test environments

Last minute changes meant this happened while some of us were in Peppa Pig world

# LUDICROUS MODE

## We were ready to go

The tools dashboard showed no medium or higher vulnerabilities after false positives were eliminated. Could we just go live without any further manual tests and checks ?





Reference to a car maker or an 80s movie are just for reference to speed

# RECAP

## TIPS AND LESSONS LEARNT

- Senior leadership buy in needed apart from bottom up engineer education
- Security for enabling business rather than blocking
- Workload selection is important
- We knew this – cutting edge is better than bleeding edge, but if you have, don’t scrimp on the team skills
- TRUST your people and tools
- Production IS going to be different even if it’s a new platform, so test in production where you can, safely
- The red pen test team HAS to be a completely independent and be objective
- Everything as code and cattle are only useful if you have tested them in production

# WHATS NEXT

**The obstacles of past are now like fun driving an off-road vehicle**

1. Development teams now use threat modelling and SAST tools to pre-empt security threats, identify risks, supply chain attacks, internal threat vectors with the anti-virus solution and more.
2. We demonstrated that the north star  of a “release in a day” does not need to compromise on security and is being used
3. From old school > Zero Trust > Cybersecurity Mesh
4. Paradigm shift from security being blockers to enablers changing negative connotations

# CONTINUING THE JOURNEY

## Can application teams go faster... with security in hand?

Application development thrives on speed, but as teams embrace cloud, agile, and DevSecOps, **security is often left behind as it's too slow and inefficient**.

**48%** of developers **don't have time** for security issues they believe are **important**.

## Application Security doesn't have to slow teams down.

- **Find critical issues**
- **Accelerate remediation**
- **Operate at scale**
- **Prioritize actions**

## When it's built for speed and scale.

**Application Onboarding At Scale**

Enabled through automated workflows.

**Automated, Meaningful Scanning**

Enabled through properly configured scans and automated, consistent execution.

**Focused, Triaged Results**

With automated filtering and decision processes to reduce false positives 50-80%.

**Clear, Actionable Reports**

Automatically generated and integrated with threat & vulnerability management systems.

**Automated Remediation**

Detailed guidance and program management, with option for automated remediation (self healing)