DevSecOps accelerator for cloud-based digital services

Expert support to build a DevSecOps capability within an organisation. We ensure security is built in from inception and throughout development into production and decommissioning of cloud-based services. Incorporating security into agile working practices using lightweight, pragmatic approaches suitable for continuous delivery. Our approach empowers teams and reduces risk.

DevSecOps is an agile, pragmatic way to develop and operate secure services. It embeds automated security checks in the deployment pipelines, and treats security as code. DevSecOps includes threat modeling, code reviews, risk analysis and penetration testing into a repeatable, measurable process. Our accelerator service supports the in-house team in building a culture of security by default.

Features

- Establishes best practice for continuous security
- Implements security testing approaches, eg. static analysis and dynamic testing
- Delivers a centralised vulnerability management system
- Creates a security community of practice within the organisation
- Trains and mentors developers to become security champions
- Trains delivery teams in secure software delivery and operation
- Implements agile threat modelling
- Develops security operations capability
- Implements security incident response procedures
- Brings technical security expertise to DevOps

Benefits

- Improved security without blocking delivery
- Delivers a quantifiable improvement in security
- Helps teams take ownership of the security of their services
- Identifies security issues as early as possible
- DevSecOps explained by experts using plain English
- Proven track record supporting DevSecOps adoption within government
- Consultants experienced in meeting GDS and NCSC guidance
- Recommends pragmatic approaches to security

- Improves quality of external penetration testing exercises
- Drives better decision making on security budgets

Our service is recommended for any public sector organisation embarking on cloud technology adoption and usage, with the consequent need to plan for the secure development, testing, deployment and operation of cloud-based digital products and services. It is also recommended for organisations that have existing cloud infrastructure or software in place but who are concerned with the security practices followed in delivering those services.

Our security consultants carefully analyse existing security practices, for example:

- automated security testing
- threat modelling
- risk analysis
- code review
- static code analysis
- dynamic security testing
- penetration testing
- security monitoring

They then produce guidance and recommendations on how to effectively and efficiently build security into the agile delivery practices of the delivery teams.

Our DevSecOps Accelerator service builds an in-house DevSecOps capability, growing these capabilities and skills with existing staff or helping to define job descriptions and recruit staff for the security team. We bootstrap security capabilities by working closely with client staff to train and equip them with the tools they need to ensure security is effectively adopted across all the delivery teams.

We help to improve agile security practices, leverage continuous delivery to reduce risk and improve the security posture of the organisation. Our security experts provide proven strategies for incorporating security into agile working practices using lightweight and pragmatic approaches, including automation techniques, that measurably improve security in continuous integration and continuous delivery pipelines. Our service helps ensure clients can manage risk effectively within the Shared Responsibility Model of the cloud provider that has been selected.

Our security consultants have in-depth, hands-on experience and expertise in building strong security communities of practice within a diverse variety of organisations and

industries, including government, finance, banking, retail, and many others. Our consultants have first-hand experience in how security works best within agile environments, and how to match corporate security, compliance and risk management with modern iterative delivery practices focused on rapid release to production.

Our approach to DevSecOps acceleration

Equal Experts consultants are highly experienced in modern agile and lean practices. They bring with them experience of a wide range of business domains and industries, including many industries that face strong regulation around security, such as banking and finance. They excel at communicating with senior stakeholders and delivery teams across an organisation, using plain language that is easily understandable to non-security specialists.

Our approach is to assess the maturity of the organisation in building security into software and systems, using industry standards such as the NIST Cybersecurity Framework and OWASP Security Assurance Maturity Model (SAMM), as well as security industry best practices.

Our consultants analyse the current approach to security, identifying any areas of friction between corporate security policies and modern DevOps practices such as continuous integration and continuous delivery. We work with the risk management team to understand the major risks faced by the organisation, alongside common industry risks, and identify any existing security practices that are being followed to respond to those risks.

Once we have a complete picture of the current security practices, we provide an assessment of security maturity and document this based on supporting standards and industry resources, benchmarking the organisation against other similar organisations and industries.

Our security consultants then begin introducing a set of DevSecOps practices in order to improve how security is built into the software and services. These practices are risk-based, and tie directly to measurable security outcomes for the organisation. We do not believe in arbitrary scoring systems, but instead value outcomes that can demonstrably improve security through the reduction of risk. No two organisations are the same, and therefore no two DevSecOps recommendations are the same.

We will recommend particular products, where applicable, or certain feature sets that will help deliver more secure services. For example, some organisations do not have a vulnerability management system designed to support continuous delivery or bespoke software development. In cases such as these, we will recommend various approaches to address the gap either through procurement of commercial software, adoption of open source software, or building custom software to address the requirement.

All of our recommendations are based on products or capabilities that we know to be effective for organisations that have adopted agile delivery techniques and tools. We value automation and integration capabilities, as we believe that many of these features must be tightly integrated into build pipelines in order to be most effective.

Our consultants work to improve development and operability practices, ensuring that security is considered throughout the lifecycle of the service. We review security monitoring operations and identify any areas that can be improved in order to bring security and development teams closer together.

As with DevOps, DevSecOps is more about organisational culture and mindset than about any specific technology or technique. A fundamental part of our service is explaining and demonstrating this culture and mindset to all those involved in the delivery of services, from senior management to development teams, in order to give an organisation the best chance of success in secure software delivery.

Examples of DevSecOps in action

A team of Equal Experts security consultants have implemented DevSecOps for a major UK government department, which operates a large microservices architecture running in the cloud supporting hundreds of microservices.

After examining the existing security practices within the department, our security consultants identified a number of areas where improved focus on security would yield measurable benefits to the organisation. We produced a backlog of themes (such as “Application Security”, “Platform Security”, etc.) and epics (such as “Static Analysis”, “Dependency Checking”, etc.) and ranked these based on value to the organisation and security impact. Those items that were determined to have the highest value and impact were tackled first. For example, dependency checking might be a high value exercise that can be rolled out very quickly with low disruption to delivery teams, yielding great impact in a short space of time; whereas other epics might require more direct involvement with delivery teams and be slower to roll out with lower impact.

While rolling out improvements in DevSecOps practices across both the platform and the microservices than run on top of it, the team also provided security consulting to delivery teams in order to improve the security capabilities within each delivery team and foster collaboration between security and development. This proved to be an excellent avenue for identifying and encouraging security champions across the organisation, which helped scale the supply of security expertise to better meet demand.

Our team took the lead in security incident response, providing a clear procedure to be followed together with a documented and agreed risk triage framework. This framework provided a barometer for measuring the most appropriate response for a given incident, reducing the tendency to either under- or overreact to security incidents. We also managed the communications between varying stakeholders including senior management, delivery teams, corporate security and information risk teams, and the departmental CISO.

The biggest challenge in this project was in scaling supply to meet demand, particularly as we were supporting more than 50 delivery teams working in geographically dispersed locations. To address this challenge, we focused on three main activities:

- Building automated security testing tools that were easy for teams to adopt (or automatically included) in their build pipelines
- Improving platform-level security features, such that all teams and microservices would benefit from the improvements with little to no change to their services
- Consulting with teams working on higher risk projects and training them to perform their own threat modelling and security reviews wherever possible

Through these activities, we were able to demonstrate improved security across the platform through:

- Improved day-to-day secure delivery practices followed by teams across all locations
- Improved response time for security incidents, including more thorough and methodical vulnerability analysis and management through to resolution
- Improved security awareness and enthusiastic participation from delivery teams
- Collaborative support between teams on security issues
- Automated, test-driven approach to security vulnerability resolution

Team

We are different. Equal Experts is a global community of 500 permanent staff and 4000+ associates, including ~800 active independent consultants and ~1200 alumni, many of whom are happy to return when we have projects and our clients need them.

We have grown organically, mostly via personal referrals, looking for quality, experience and cultural fit above all else. After a rigorous selection process, experts are added to our network, whether we need them immediately or in the future.

90% of our consultants have >12 years of experience (average >18 years) in development, delivery, operation and maintenance of digital services using agile methods. Many have significantly more and in some cases are global influencers. Their maturity and pragmatism means they are highly collaborative, happy to transfer knowledge and keen to help clients build internal capability.

Our standard working model for teams is hybrid remote first/onsite, with a core generally located in proximity to client offices, minimising travel costs and environmental impact. This ensures they can be onsite for workshops, meetings, and onboarding activities, and can work collaboratively with client team members, stakeholders and other suppliers. In the words of one client ‘your consultants leave their Equal Experts badges at the door’.

Roles

Collectively, our consultants have the multi-disciplinary experience and expertise needed for successful transformation to cloud-first delivery, live service maintenance and new operating models. Our network means we have fast and flexible access to the skills our clients need. We have specialists in all areas needed for digital success, including:

- Delivery managers
- Change managers
- Product managers
- Engagement managers
- Strategic advisors
- Security specialists
- Data scientists
- Data engineers
- Data architects
- Technical leads

- Technical architects
- DevOps consultants
- Developers
- Testers
- Business and performance analysts
- Accessibility experts
- Service designers
- User experience designers
- Content designers
- User researchers

If a client needs other specialists or niche skills, we can rapidly and confidently engage with other organisations in our established ecosystem of proven partners. Each consultant is interviewed by EE to ensure a high level of knowledge before we provide them to clients.

Public sector clients

We know what it takes to implement and support cloud-based applications within complex public sector organisations and across large multi-vendor programmes. We understand and adhere to the GDS digital service standards for delivering solutions and handling and securing data within critical national systems. We have experience in consulting, deploying and supporting solutions that are security accredited and have passed many standard GDS assessments. Many of our consultants have active SC clearance level (some have DV) as they have previously worked with public sector clients.

Equal Experts has helped implement digital services to government digital service standards (including passing many formal GDS service standard assessments) for:

- His Majesty's Revenue and Customs (HMRC)
- Ministry of Justice and His Majesty's Prisons and Probations Service (HMPPS)
- Department for Work and Pensions (DWP)
- His Majesty's Passport Office (HMPO)
- Department of Health and Social Care (DHSC)
- Department for Environment, Food & Rural Affairs (DEFRA)
- Department for Business, Energy & Industrial Strategy (BEIS)
- Home Office
- Border Force
- Department for Education (DfE)
- Registers of Scotland

- Office for National Statistics (ONS)
- Civil Service Recruitment
- Coal Authority
- Intellectual Property Office (IPO)
- His Majesty's Courts and Tribunals Service (HMCTS)
- States of Guernsey
- Cabinet Office
- Government Digital Service (GDS)
- Valuation Office Agency

Why choose Equal Experts?

Equal Experts' diverse teams of talented, experienced software consultants bring maturity, pragmatism and passion to software products and services of all shapes and sizes. We support end-to-end delivery, deployment, migration and maintenance of elegant, bespoke applications to the cloud and provide all the services that making them entails. This includes everything from mobile apps to enterprise-level technology platforms and digital transformation to client capability building.

Since our inception in 2007, we have sought out quality above all else. We are adept in all agile and lean practices, for example:

- close collaboration
- rapid feedback loops
- keeping it simple
- empowered teams
- test automation
- continuous integration and delivery
- pairing
- refactoring
- constant learning and improvement
- learning by doing
- continuous improvement

Our focus on senior talent means that all our consultants have the skills and experience required to thrive in dynamic, challenging client environments. It means we can focus on work that adds real value, rather than micro-managing more junior consultants. Our non-hierarchical structure also allows us to operate with lower overheads.

For our teams, this creates a mature, pragmatic and innovative working environment, somewhere they can implement the best solutions of their already distinguished careers. And for our clients, it translates to better services, delivered faster and at lower overall cost. We were ranked 4th in Glassdoor's Best Places to Work 2024 and 15th in Newsweek's Most Loved Workplaces 2022.

It also means our people have the expertise and consultancy skills to help transfer knowledge of new ways of working to our client's team members, helping to build their internal delivery competency and capability.

Equal Experts' approach has a successful track record of delivery across the private and public sectors. Our award-winning deliveries include HMRC's Multi-channel Digital Tax Platform, chosen as the British Computer Society's Digital Project of the Year, and the Home Office Visa Application service, Computer Weekly's Best Public Sector Project.

Equal Experts has Business Units in the UK (London and Manchester), USA, South Africa, EU (Germany), Australia, and India.

We're proud to be one of the top suppliers to the public sector via the G-Cloud and DOS frameworks. Our services are also available through RM6100 Technology Services (Lots 1, 3d) and RM6263 Digital Programmes and Specialists (Lot 1), RM6195 Big Data and Analytics (the only supplier on all 6 capabilities) and RM6335 DALAS (Lot 2a), and various DPS Frameworks, including RM6094 Spark, RM6173 Automation Marketplace and RM3764 Cyber Security.

For more information and case studies, please visit https://www.equalexperts.com/ or contact us at solutions@equalexperts.com.

Planning

To build detailed knowledge of the context and domain for any project, an initial phase of planning, definition and knowledge transfer will generally take place at the start of an engagement.

We have found that this takes place most effectively through a short time-bound inception to develop a shared understanding and agreement on vision and objectives across a broad stakeholder group. This covers the business, technical and user aspects of the project and the outputs may include user personas and scenarios, key user journeys, as-is and desired business processes, a prioritised backlog of user stories, technical constraints and vision, and a release roadmap and plan. The techniques and principles applied are

also used on an ongoing basis throughout the course of delivery, to ensure the solutions developed are fit for purpose and meet real and changing user needs.

This initial inception phase can be contracted separately if required.

Setup and migration

In addition to ongoing development and operation of live cloud-based services, we can help with the initial set up and migration as part of a transition to cloud. We look for opportunities to automate processes (for example, test, deploy) that will yield real benefit and high ROI. Our approach helps to address integration, dependencies and risk early. We capture actionable metrics to measure and manage progress towards meeting the agreed success criteria and KPIs identified for building and operating the service. The highly collaborative, interactive processes we follow foster continual learning and improvement of services. They help to establish and evolve the overarching service design, management processes and the team capabilities.

We can ensure projects hit the ground running through our experience in designing, configuring and setup of many continuous delivery and automated cloud deployment environments. These techniques allow software to be repeatably and reliably deployed and tested through each stage into production on the cloud. We have substantial experience when it comes to the tooling required for continuous delivery and automated software deployment, greatly facilitating the software set up, build and migration process, which increases programme productivity and reduces project risk and cost.

Quality assurance and performance testing

All our consultants have extensive experience of both manual and automated testing, including performance testing, continuous integration and delivery into production environments at scale. With all clients we actively encourage the adoption of robust and meaningful automated test coverage, delivery and test techniques, to reduce risk and safely increase delivery velocity. We are happy to work with a clients existing quality management system (QMS) where appropriate.

Security services

We hold ISO9001:2015 Quality Management System, ISO27001:2017 Information Security Management System, Cyber Essentials (IASME-CE-018168) and Cyber Essentials Plus (IASME-CEP-003763) certifications.

We can provide the following security services if required:

- Security strategy
- Security risk management
- Security design
- Security incident management
- Security audit services

Training

For every client, we aim to transfer and embed knowledge of technology and process innovation. Our consultants help improve our clients' internal competencies and build long-term sustainable capability, as they migrate to modern cloud-based products and services. We tailor particular practices to address specific organisational constraints – we recognise that every organisation is different and there is no "one size to fit all".

The depth of experience of our consultants means they are mature, pragmatic, and have an approach grounded in hands-on digital experience. This is key to our ability to help with training, upskilling and building knowledge of new ways of working within client team members. All our consultants are selected based on their demonstrated understanding of how intelligent and innovative uses of technology are being put to work to provide competitive advantage across industries. Passing this expertise and understanding to our client team members is a key, and unique, advantage and value provided throughout our engagements.

We tend not to offer classroom-based training as our consultants are happy to share their knowledge throughout a project. They take responsibility for helping individual client team members adopt new practices and ways of working.

Ongoing support

Our operational philosophy is "you build it, you run it'". The delivery team responsible for the development of a live service usually also takes responsibility for its operation. We have found that development teams which support their own products are motivated to deliver higher quality, more robust and maintainable code.

When a service is live with real users we expect the delivery team to provide 2nd line (infrastructure, in conjunction with hosting support agreements) and 3rd line (applications) support during business hours. We can agree an appropriate model for 24/7 on-call

coverage if required - see our G-Cloud On-Call Support offering for details. We typically establish an on-call rota with delivery team members assigned on a weekly basis.

Our experience is that digital services are never really finished and that it is important to retain some level of investment to allow the addition of new features as the needs of customers (both internal and external) change. Our design of the end-to-end service can include establishing Service Level Agreements for ongoing service evolution and operational support (ensuring agreed levels of service availability).

User support

We provide an engagement manager on all G-Cloud engagements with responsibility for ensuring customer objectives are met, and for addressing any issues with service delivery. Our engagement managers act as an escalation point, and can be reached via phone or email, to respond to issues beyond the control of the team providing the service. Engagement management is included within our service pricing.

When a service is live with real users we expect the delivery team to provide 2nd line (infrastructure, in conjunction with hosting support agreements) and 3rd line (applications) support during business hours. We can agree an appropriate model for 24/7 on-call coverage if required - see our G-Cloud On-Call Support offering for details. We typically establish an on-call rota with delivery team members assigned on a weekly basis.

Social Value

Tackling economic inequality Theme 2 MAC2,3

ENTREPRENEURSHIP AND TRAINING

For GCloud contracts, we will:

- Flow ~65% of revenues to our Associate supplier network (small, entrepreneurial businesses).
- Expand and assign consultants from EE's Evolve programme, which mentors technology practitioners to become expert consultants.
- Work with specialist partners (eg. SigmaLabs, NorthCoders) to develop skills for under-represented and early-career candidates, assigning them to our teams and using our expert consultants to coach and train them.

- Provide retraining and return opportunities, mentoring, development of technical skills which address skills gaps, training through mock-up interviews, provision of CV and careers guidance.
- Where possible, provide opportunities to employ and develop more people with protected characteristics in new skills relevant to the contract.
- Share knowledge and experience publicly via ExpertTalks and Open-Source Playbooks to develop disadvantaged groups' skills.
- Partner with leading diverse communities, networks and ambassadors to identify suitable candidates eg. SigmaLabs, Coding Black Females.
- Continue hosting events for minority and under-represented groups, for example, 10 Digital Ladies and Women Who Code.

DIVERSE SUPPLY CHAINS

Our partnering model directly supports SMEs and SEs, which we engage as specialist subcontractors. We identify new businesses, entrepreneurs, start-ups, SMEs, VCSEs and mutuals that can participate in our supply chain and those of our clients.
For G-Cloud contracts, we will:

- Procure in a fair and open, PCR2015 manner.
- Establish innovation programmes to identify and onboard new micro businesses.
- Encourage suppliers to diversify their supply chain in line with our goal to increase supply chain resilience.
- Increase supply chain governance using recognised bodies such as sedex.com.
- Measure and increase staff characteristics and success in our associate/supplier diversity (eg. %spend with each supply group across micro, SME and collectives; %of start-up suppliers still in business after three years).

Fighting climate change Theme 3 MAC4

Equal Experts has a robust Environmental Policy, aligned with PPN06/20 Theme 4, PPN06/21 and the UN Sustainable Development Goals, which details commitments to reduce our environmental impact holistically across the organisation. We have published and updated our plans annually since 2019, meeting the government's Streamlined, Energy and Carbon Reporting legislation (SECR), initially reporting Scope 1 and 2 emissions. Our Carbon Reduction Plan is published on our website and has been certified to meet PPN06/21 requirements by CCS.

EE is committed to achieving net-zero Carbon emissions by 2030. We are actively exploring investments in innovative, effective carbon-offsetting initiatives to achieve this target. Our internal Carbon Net-Zero Governance working group advises the Exec Team on meeting the 2030 net-zero target.

For G-Cloud contracts, we will:

- Build systems making extensive use of cloud services. Most systems we build use automated scaling of resources to ensure we minimise both cost and environmental impact of operation. We migrate to more efficient resources and operational practices as cloud providers introduce them.
- Encourage and support remote and hybrid working, and provide access to tools like Zoom, Lucidchart and Miro to encourage and facilitate this and thereby reduce our carbon footprint. We have written an open-source Remote Working Playbook which is available to anyone via our website.
- Assign local staff to client engagements whenever possible, to reduce travel impact.
- Use flexible co-working spaces with high BREEAM ratings.
- Reduce office material consumption and waste eg. printers and paper, recycle and reuse wherever practical.
- Reduce energy and water consumption.
- Consider the environment in our branded merchandise used at events and promotional activities, particularly reducing plastic use and local sourcing.
- Improve our recycling efforts, particularly IT equipment (our largest relevant expenditure in this area), and deliver social benefits through reuse wherever possible.

Equal opportunity Theme 4 MAC5,6

EQUAL OPPORTUNITIES

Equal Experts has a longstanding commitment to advancing diversity, equality and inclusion. We operate in ways that support clients to deliver their Public Sector Equality duty under section 149 of the Equality Act 2010. We are Level 1: Disability Confident Committed and members of the Business Disability Forum.

For G-Cloud contracts, we will:

- Run monthly team psychological safety surveys, share results with teams, help teams identify and support improvement actions.
- Invest in workshops and training to help teams improve safety and inclusion.
- Host events for minority groups, such as 10 Digital Ladies and Women Who Code.
- Provide family-friendly and dignity-at-work policies (we were placed 4th in Glassdoor's Best Places to Work 2024).
- Continuously evolve recruitment processes to improve diversity, equality and inclusion, and provide unconscious bias training for our recruitment team.

- Engage Druthers, executive search specialists in building inclusive teams, to broaden our team diversity.
- Where possible, provide opportunities to employ and develop more people with protected characteristics in new skills relevant to the contract.
- Make appropriate adjustments where practical to support and develop individuals with physical, mental and hidden disabilities.
- Regularly monitor our performance (eg. Cabinet Office CAESER, B Impact Assessments) to help develop annual improvement plans.

MODERN SLAVERY

EE is covered by the Modern Slavery Act 2015. Our published policy statement, processes and procedures are reviewed and updated annually (eg. Employee Team Charter, Whistleblowing Policy, Code of Conduct for Suppliers).

We will undertake due diligence when considering taking on new suppliers and regularly review existing suppliers. This includes evaluating modern slavery risks. We are members of Sedex Global and will use their services to review our extended supply chains and provide confidence to our clients.

Wellbeing Theme 5 MAC7,8

HEALTH AND WELLBEING

Equal Experts promotes psychological safety, trust, inclusion and a “grown-up” culture throughout our workforce. We work closely with our clients to support the health and wellbeing of our team members, establishing onboarding practices and developing local team charters to ensure new team members are welcomed and made to feel safe. We support the six standards of the Mental Health at Work Commitment and the Race at Work Charter and encourage our supply chain to do the same.

For G-Cloud contracts, we will:

- Run monthly team psychological safety surveys, share results with teams, help teams identify and support improvement actions.
- Promote inclusive and accessible recruitment and retention practices to ensure people feel valued (Equal Experts was placed 4th in Glassdoor’s Best Places to Work 2024).
- Offer flexible and remote working and encourage staff to take regular breaks, “Movement Snacks” (workstation exercises), holidays, online team-events.
- Provide awareness training and guidance through our policies, ExpertTalks and playbooks.

- Offer private medical cover for our UK employees and their families, including encouraging exercise and other preventative measures.
- Host public online ExpertTalks on Health and Wellbeing, eg. “Avoiding Burnout”.

INTEGRATED COMMUNITIES

For G-Cloud contracts, we will:

- Foster an open, inclusive working culture eg. 'no-blame' retrospectives to help us learn from each other's perspectives.
- Hold socials and lean coffee sessions to ensure a welcoming culture that leads to better team bonding and working relationships.
- For physical health, hold our annual Walkathon competition for staff and family members, clients and partners, which encourages physical activity and raises money for charity (1200 participants, £136k raised in 2023).
- Encourage companies in our supply chain to implement measures to improve employees' physical and mental health and wellbeing, and implement standards in the Mental Health at Work commitment.