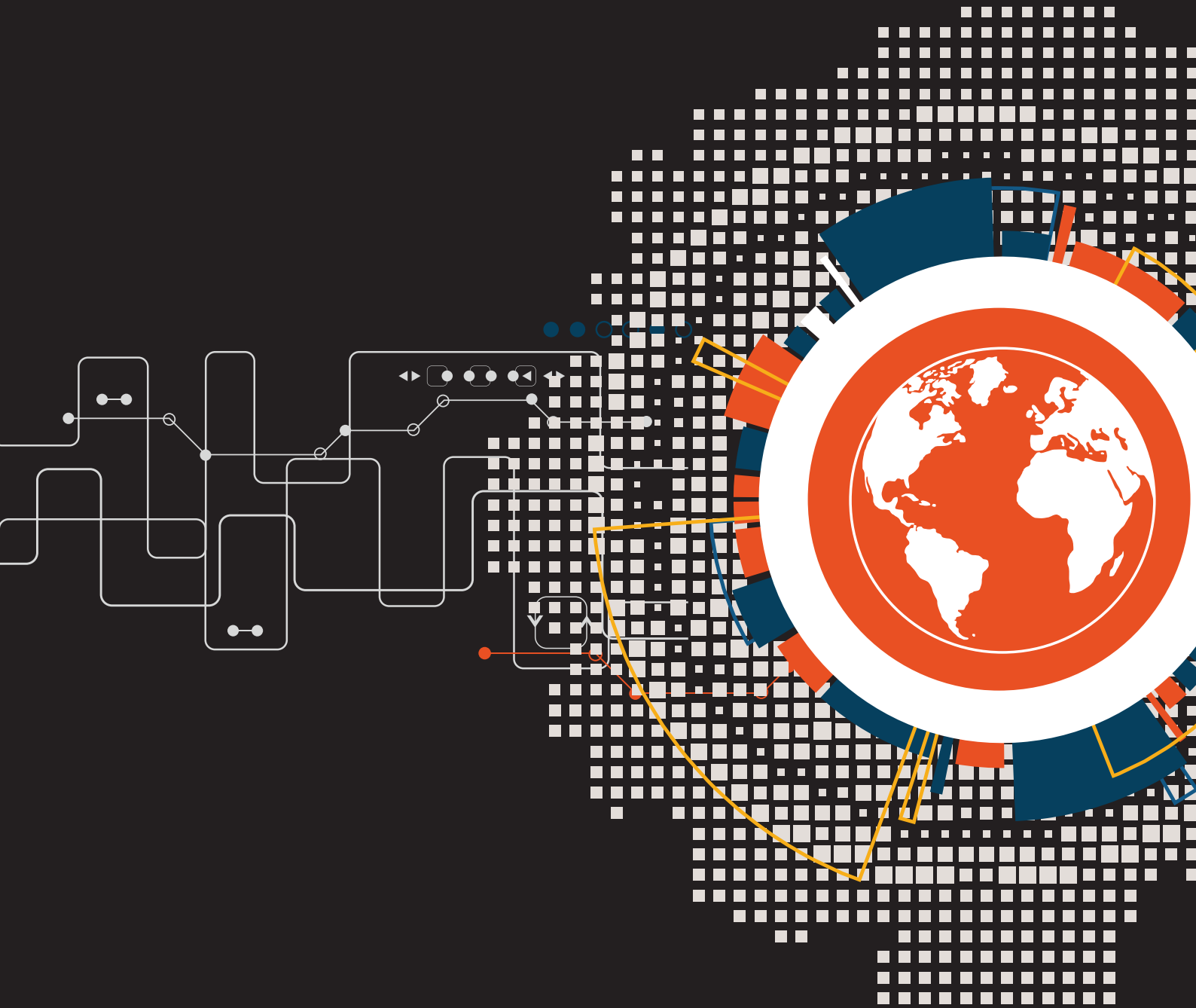


boesystems.com/securecloud

Helping Secure Government Organisations Apply DevSecOps



BAE SYSTEMS

For nearly a decade, new working practices and operating philosophies have been transforming the way engineering teams can rapidly deliver secure new applications within increasingly digitally based organisations. To do this effectively requires a working knowledge of modern engineering practices combined with a thorough understanding of an organisation's mission, working environment and challenges.

Due to security concerns, some secure government organisations have been slower to leverage the benefits of the cloud than they would have liked, and they continue to follow outdated engineering methodologies. However, having already successfully implemented and effectively transformed engineering practices within a number of Secure Government organisations, BAE Systems believes the benefits of modern engineering delivery methodologies such as DevSecOps should be available for all secure organisations. We understand that there is no 'one-size-fits-all' approach to different customers: each is different. We also understand that when working with established engineering teams, winning hearts and minds can be difficult and that people can be resistant to change. Over the past few years we have successfully helped many secure government organisations migrate to a DevSecOps methodology and benefit from the agile development of new applications and systems to carry out their mission, securely and faster – including those who work across siloed, protectively marked networks.

A Quick Guide to DevSecOps:

Under DevSecOps ways of working, Security experts, Development and IT Operations teams are combined into a single homogenous engineering team which is responsible for the unified creation, delivery, security, enhancement and sustainment of applications or services throughout the entire software/service lifecycle.



Our Differentiator: Security, understanding our customers' missions, and proven experience

For secure government organisations wanting to transform their engineering practices it's important to find the right partner: it needs to be an organisation that not only lives and breathes the 'security' implicit at the heart of all DevSecOps operations, but who also has intimate knowledge of the challenges, working environments, culture and operational drivers of government organisations.

On a day-to-day basis, our global teams work within Government organisations, helping transform legacy engineering and support groups into modern, agile, high-performing teams. From our experience, key considerations for successful DevSecOps operations are:

In 2019, BAE Systems had over 40 DevSecOps teams and over 250 engineers that delivered over 650 sprints into UK Secure Government customers.



Understanding, living and breathing the mission of our customers: For decades our teams have been working within secure government organisations, deeply embedded, committed, and passionate. We've accumulated hundreds of work years understanding why and what our customers do, and how they do it.



The importance of security cleared staff: Strict vetting rules will apply to the individuals who make up any teams. BAE Systems has a large pool of Suitably Qualified and Experienced Personnel (SQEP) who are already vetted and security cleared.



Adopting a threat based approach to achieving the balance between security and agility: At no stage should the risk of such developments threaten the security of the government organisation and the data it holds. We adopt a threat-based approach to risk that informs which additional security controls and accreditation may be required to mitigate identified risk and how to include them from the outset.



A mix of low and high side working: Government organisations are increasingly adopting a 'develop-low, deploy-high' working practice, where new applications are built and tested in a low-side, Official, development environment, before deployment to the high-side, i.e. protectively marked networks. BAE Systems has extensive experience in working with customers in this manner, with hundreds of engineers supporting low/high side environments on an ongoing basis. For more information please see our brochure "Helping Secure Government Organisations establish integrated Low-side/High-side working practices."



Automating Secure Development Environments for Secure Government Organisations: We are developing automated toolkits to rapidly instantiate secure, accredited environments which automatically encapsulate appropriate security controls as part of the backbone of application development pipelines.



Knowledge Sharing: At regular intervals, our engineering teams are rotated between departments. This enables teams to both share best practices with other departments and to increase their own knowledge, expertise and exposure to the challenges and issues of different areas.

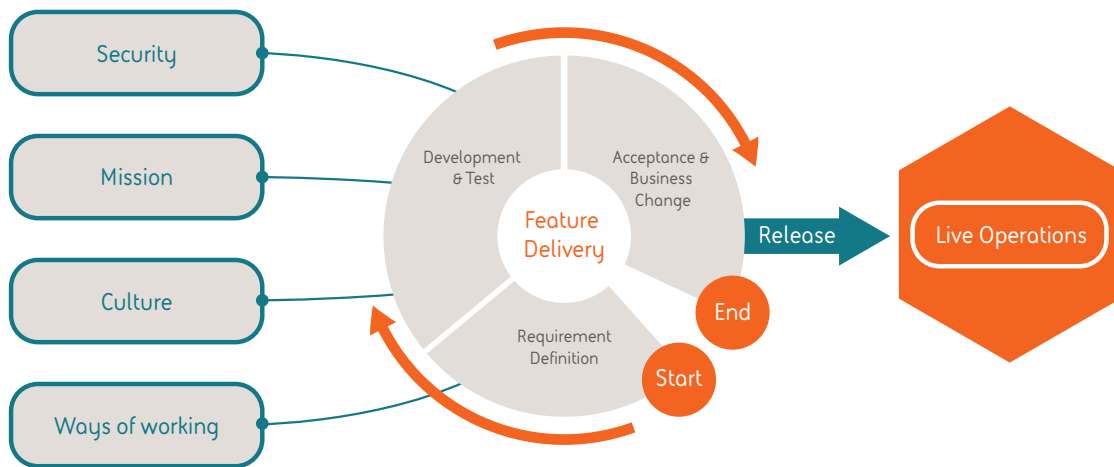


Figure 1: Successful DevSecOps delivery within a Secure Government department requires a close understanding of the mission, ways of working, security procedures and culture of the department.

Summary: The Value of Experience:

Secure Government organisations need partners that they can trust to deliver amidst the most demanding conditions, and often under great pressure. When it comes to implementing large scale business change, government organisations need to have the assurance that their DevSecOps teams will do it right and get the job done. To do this, organisations need a trusted partner who understands their unique challenges and who has done it all before. BAE Systems has.

To learn about more about how we can help you develop high-performing engineering teams within your challenging environments, please contact us at learn@baesystems.com.

We are

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology, defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
Level 1
14 Childers St
Canberra
ACT 2601
Australia
T: +61 1300 027 001

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/securecloud

 linkedin.com/company/baesystemsai

 twitter.com/baesystems_ai

Copyright © BAE Systems plc 2020. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ. No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Applied Intelligence.