Capgemini

DevSecOps
G-Cloud 14

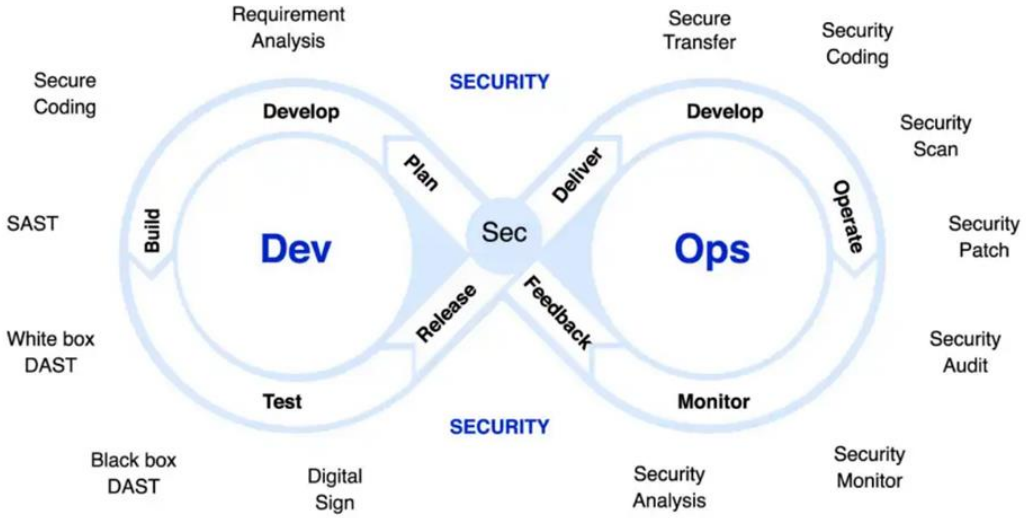
November 2024

Table of Contents

1 Service Overview

DevSecOps is a security enabled DevOps that emphasizes an early integration of secure culture, tools, and practices into each phase of software development life cycle. This empowers large companies to enhance their security posture and shield themselves from cyber-attacks while expediting software development by integrating security practices into the software development lifecycle. As a leading provider of DevSecOps services, Capgemini has over 500 security professionals based in the UK who can be leveraged to delivers top-tier experts and rigorous quality assurance procedures to help businesses stay ahead of the ever-evolving threat landscape.

Capgemini's DevSecOps service integrates security practices into the development lifecycle, ensuring robust protection for software systems. By combining industry standards such as NIST guidelines and OWASP (DSOVS) with cutting-edge automation tools and collaborative methodologies, we enable our clients to prioritize security without hindering development speed.



This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini

2 Business Need

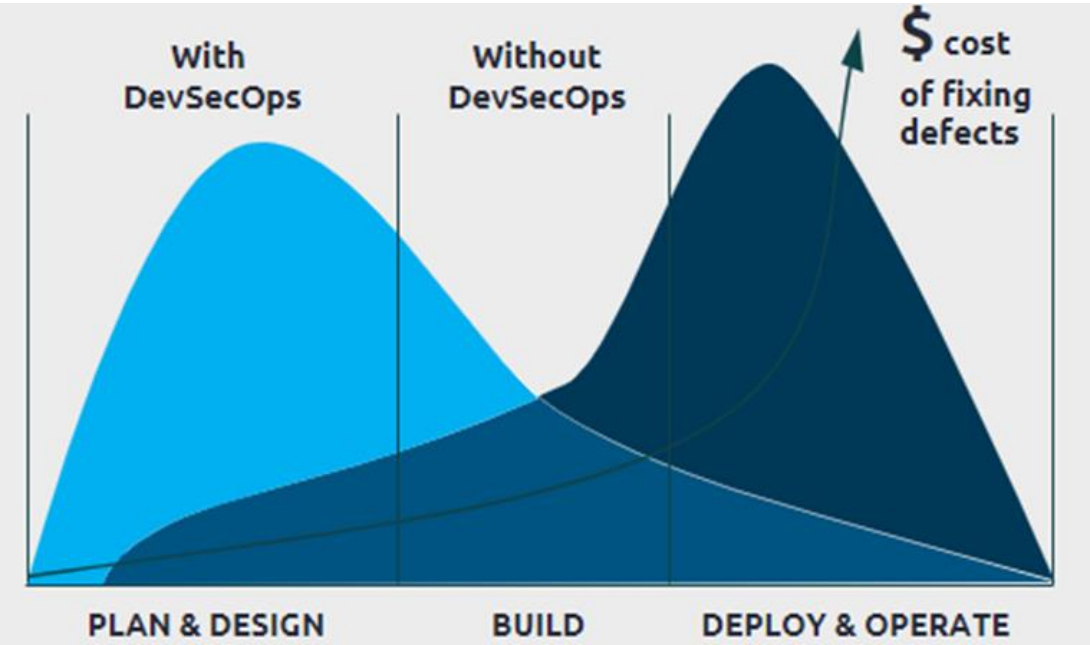
In today's rapidly evolving digital landscape, businesses face increasing threats to their software systems. Traditional security measures are no longer sufficient to protect against sophisticated cyber-attacks. Organizations require a proactive approach that embeds security into the development process from the outset. Our DevSecOps service addresses this needs by providing continuous security assessment, real-time threat detection, and seamless integration of security practices into the DevOps workflow.

The benefit of security embedded throughout the CI / CD pipeline is that engineers are incentivised to continuously consider security though multiple cycles of development. This avoids finding risks in the final stages of the SDLC, which can be very costly, and encourages a culture of collaboration between security and development.

The following are why DevSecOps is needed;

- Cost reduction by detecting and fixing security issues during the development phases.
- Improve speed of delivery by minimizing security bottlenecks and rework.
- Enhance speed of recovery by utilizing methodologies when security incident occurs.

- Improve threat hunting that reduce reputational damage.
- Ensure Security by using automated security review of code.
- Empower developers to use secure design patterns.



This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini.

3 Our Approach

Drawing from our extensive work with major public sector, financial service, logistics and global hospitality entities, proficiency in cloud integration, and comprehensive utilization of industry-standard frameworks, Capgemini is proficient in guiding clients towards the optimal approach tailored to their individual business requirements.

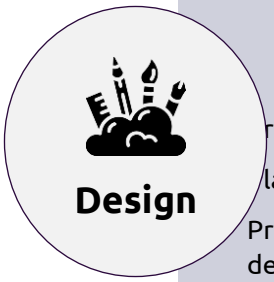
Our service is provided in a 3-Step streams of activity that addresses DevSecOps Framework:

Discover

Rethinking DevSecOps Enablement

M.A.C.E. Framework

- Review culture, processes and tools to provide a set of recommendations to shorten release cycle.
- Assess existing maturity of organization's development using Capgemini's M.A.C.E.



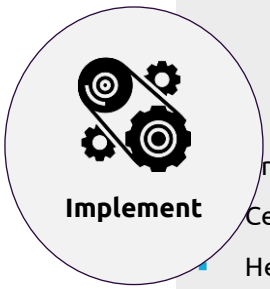
An Efficient Agile Architecture

Security Testing

reate basic building blocks and best practices for DevOps enablement.

lan and track work using agile methodologies.

Promote a culture of collaboration between business decision-makers and application development teams.



Facilitate the Knowledge on Tools, Culture and Competencies

Security Dashboarding

rovide KPI and Synthesis

Centralize testing.

- Help to prioritize.

3.1 Discover

3.1.1 DevSecOps Maturity Assessment Approach

- Cover Six Dimensions of DevOps:
  - **Planning and Process** to prepare for projects and releases.
  - **Source Control** to manage the code.
  - **Development and Testing** to use methodologies and frameworks.
  - **Build and Release** to build the code and manage through environments.
  - **Deployment** to deploy the code.
  - **Monitor/Measure** to measure success of development lifecycle.
- Identify Strengths, Weaknesses, Opportunities, and Threats
- Generate a Maturity Score.

3.1.2 DevSecOps Threat Modelling

- Reduce the time taken to derive security requirements from days to minutes.
- Reduce the time and resources required to perform risk analysis.

- Meet enterprise security requirements and constraints from the very beginning of the SDLC.
- Manage security risk throughout the SDLC by choosing a risk response and synchronizing security requirements with issue trackers such as JIRA.

3.2 Design

3.2.1 Static Application Security Testing (SAST)

Initial Assessment & Scoping

- Understand business requirements and design specifications.
- Understand application functionality.
- Prioritize critical applications based on compliance mandates and application criticality per customer.
- Integrate SAST into CI/CD pipeline.

Code Review

- Perform static analysis using code scanners.
- Conduct manual verification to eliminate false positives.
- Perform manual code review for the languages not supported by tools.

Perform Open-source Code Scan

- Scan for vulnerabilities in the open-source code used.
- Identify outdated open-source libraries/binaries/components.

Prepare Code Analysis Report

- Automated analysis of application risk level and report generation
- Recommendation on how to fix identified issues.
- Generate secure code analysis report and secure code review guidelines.

3.2.2 Software Composition Analysis (SCA)

- Create an accurate Bill of Materials (BOM) for all your applications.
- Discover and track all open source.
- Set and enforce policies.
- Enable proactive and continuous monitoring.
- Integrate open-source code scanning into the build environment seamlessly.

3.2.3 Dynamic Application Security Testing (DAST)

Identifying the Scope & Goal Definition

- Identify scope of Web application Penetration Test
- Understand application purpose and function.
- Define success/exit criteria.
- Integration of DAST in CI CD pipeline after build change

Security Assessment

- Identify vulnerabilities using automated scanners.
- False positive elimination
- Identify flaws in authentication and authorization mechanisms.
- Active and Passive scan modes.
- Exploit vulnerabilities using CI/CD Embedded Security Testing tools.

Reporting

- Automated analysis of application risk level and report generation
- Recommendation on how to fix identified Issue.
- Generate dynamic application security testing report and secure code review guidelines.

3.2.4 Mobile Application Security Testing (MAST)

- Continuous scan modules for mobile applications to track the vulnerabilities.
- Continuous monitoring for code updates
- Instant and actionable reporting

3.2.5 Results Analysis

- Results analysis from CSV + PDF report or directly on the tenant for SaaS platform
- Export of a new CSV (result of analysis, false positive removal) or update of issues including comments directly on the application tenant
- Provide CSV export and PDF report of DAST / MAST analysis or access to Tenant Access to the application.
- Reduce fix time from hours to minutes.
- Facilitating de-duplication of scan results.

3.3 Implement

3.3.1 Runtime Application Self-Protection (RASP)

- Documentation on confluence
- Automated applications monitoring and health checks.
- Automated housekeeping and archival for applications
- Change Management for NPEs
- Implement SCM with branching strategy.
- Standardize JIRA usage for projects.
- *Currently under development*

3.3.2 Security Dashboard Management

- Automated Interactive Dashboard (AID) For DevSecOps provides real-time status with real-time updates.
- Build Status
- Monitor
- Deploy
- Quality
- Code Repo
- Sprint Status
- Single Pane of Glass

3.3.3 Continuous Security Training

- Establish and educate on agile and DevOps best practices.
- Conduct ongoing training sessions for developers on
  - DevOps Tools that are compliant with security gates
    - Languages that are used for security solutions.

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The Buyer responsibilities as part of this service are as follows:

- The Buyer will define the scope of the area to be assessed.
- The Buyer will provide any training and awareness education to the security assessor as is required by the on boarding requirements.
- The Buyer will provide a project manager to act as a single point of contact and an escalation route for the full duration of the project.
- The Buyer will make available appropriate subject matter experts and documentation (business and technical) to the project as appropriate to support the security assurance assessments.
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date.
- The Buyer will announce the assessment to all appropriate individuals, asset and process owners.
- All internal and external user communications will be managed by the Buyer.
- The Buyer will accept the security assurance assessments report via post assessment presentation and be responsible for managing the recommendation identified from the assessment's activity.

If these responsibilities do not match your expectations, then please contact us in order that we can explore options to vary our approach

5 Service Management

Capgemini's service can be consumed in the following deployment and delivery models, all fully managed by Capgemini. Please contact us to discuss which of these fits your requirements. These are:

- **Offshore resources**: Capgemini's consultants work from our offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Capgemini's consultants work from our UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Capgemini's consultants work on your sites, embedded as part of your team. This provides a solution for buyers that require skills augmentation and a high degree of control over the work.

6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form (including as a minimum an exit plan in line with the Call-Off Contract terms) which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Partnerships/Alliances

Capgemini are partners with Industrial leaders in Application Security Testing according to Gartner Report 2023

Veracode is recognized as a market leader according to Gartner and has won multiple awards of excellence in the last 3 years.

MicroFocus (Open Text) is recognized as a market leader by Gartner, Forrester, IDC and G2.

10 Vendor Accreditations/Awards

For the 12th year in a row, Capgemini has been recognized as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

Capgemini can provide security delivery professionals with the following industry certifications:

- NIST Cybersecurity Framework (NCSF);
- Certified Information Privacy Professional/Europe (CIPP/E);
- Certified GDPR Practitioner;
- Certified ISO/IEC 27001 Lead Implementer;
- Certified ISO/IEC 27001 Lead Auditor;
- Certified Information Systems Security Professional (CISSP);
- Certified Cloud Security Professional (CCSP)
- Certificate of Cloud Security Knowledge (CCSK)
- Certified Information Security Manager (CISM);
- Certified Information Systems Auditor (CISA);
- Certified Ethical Hacker (CEH);
- TOGAF9, SABSA and other architectural methodologies including Capgemini's own;
- IT security specific MSc or PhD;
- Membership of the Chartered Institute of Information Security Professionals (CIISec)
- Certified in Risk and Information Systems Control (CRIS)
- Computer Hacking Forensics Investigator (CHFI)

Capgemini delivery staff hold a wide range of vendor specific certifications for many types of cybersecurity tooling.

11 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

12 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

13 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

14 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

15 Termination Terms

Please refer to the Supplier Terms for this service.

16 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the Future You Want | www.capgemini.com

C14NOV23