CAREERS THROUGH MATHS: DEVSECOPS ENGINEER

JOB DESCRIPTION

A DevSecOps Engineer is a highly specialised IT professional who integrates security practices seamlessly into the DevOps (Development and Operations) lifecycle. Their primary goal is to ensure that security is a shared responsibility throughout the entire software development process, from initial code commit to deployment and monitoring in production. This is often described as "shifting security left," meaning security is considered early and often, rather than being a final gate before release. In the UK, this role is critical for organisations in regulated sectors like finance (e.g., banks like HSBC and Barclays), government (e.g., GDS - Government Digital Service), and healthcare (e.g., NHS Digital), where data protection and compliance with regulations like the UK GDPR and the Network and Information Systems (NIS) Regulations are paramount.

The daily work environment is collaborative and fast-paced, typically within cross-functional teams using Agile methodologies. Key duties include automating security controls into the CI/CD (Continuous Integration/Continuous Deployment) pipeline, managing infrastructure as code (IaC) using tools like Terraform, conducting dynamic and static application security testing (DAST/SAST), and responding to security incidents. For example, a DevSecOps Engineer at a fintech company like Monzo or Revolut might be responsible for automatically scanning every code pull request for vulnerabilities, ensuring that any new feature does not introduce a security flaw before it is merged into the main codebase.

Mathematics is central to this role, providing the logical foundation for risk

assessment, automation, and data-driven decision-making. Engineers use mathematical models to quantify security risks, calculate the probability of a breach, and determine the impact of potential threats. They write scripts and automation that rely on Boolean logic and algorithmic thinking to enforce security policies. Furthermore, they analyse vast streams of log data using statistical methods to detect anomalous patterns that could indicate a cyber-attack, turning raw data into actionable security intelligence.

HOW MATHEMATICS IS USED

- **Boolean Algebra and Logic:** This is the fundamental mathematics behind all computing and security policy enforcement. DevSecOps Engineers use logical operators (AND, OR, NOT) to create complex security rules in systems like AWS IAM (Identity and Access Management) or firewall configurations. For instance, a rule might state: "Allow access to this database (Condition A) IF the request comes from the corporate network (Condition B) AND the user is in the 'developer' group (Condition C) BUT NOT if it's outside business hours (Condition D)." In a UK context, an engineer at the BBC might use this logic to build access controls for their iPlayer content delivery network, ensuring only licensed users can access specific regional content.

- **Probability and Statistics:** These are essential for risk assessment and threat modelling. Engineers must estimate the likelihood of a vulnerability being exploited and its potential business impact. They use statistical analysis on security event logs to establish a baseline of "normal" system behaviour. Any significant deviation from this baseline, detected using measures like standard deviation, can trigger a security alert. For example, a DevSecOps Engineer at a retail company like Tesco or Sainsbury's might analyse web traffic patterns to identify a distributed denial-of-service (DDoS) attack during a high-sales event like Black Friday, distinguishing it from legitimate high traffic.

- **Algorithms and Complexity:** The efficiency of security scanning tools is governed by algorithms. DevSecOps Engineers need to understand algorithmic complexity (often expressed in Big O notation) to select the right tools for their pipeline. A SAST tool that takes 8 hours to scan a codebase ($O(n^2)$ complexity) would be impractical for a team deploying multiple times a day. They would seek a more efficient tool (e.g., $O(n \log n)$) or optimise the scanning process. When

writing their own automation scripts, they must design efficient algorithms to avoid slowing down the development process.

- **Cryptography:** While often abstracted by libraries, a conceptual understanding of the mathematics behind cryptography is crucial. This includes number theory concepts like prime factorisation (which underpins RSA encryption) and modular arithmetic. A DevSecOps Engineer managing secrets for a UK government service on GOV.UK must understand how encryption keys are generated, managed, and rotated to protect sensitive citizen data, ensuring compliance with the UK's National Cyber Security Centre (NCSC) guidelines.

- **Statistical and Analytical Methods:** Data analysis and mathematical modelling are used extensively for security metrics and compliance reporting. Engineers create dashboards that track key risk indicators (KRIs), such as "mean time to detect" (MTTD) and "mean time to recover" (MTTR) from security incidents. They use regression analysis to predict system load and potential security bottlenecks. For a UK insurance company like Aviva or Lloyd's, a DevSecOps team might build models to correlate failed login attempts with geographic IP addresses, helping to proactively block credential-stuffing attacks from high-risk regions.

KEY SKILLS & TOOLS

Skill/Tool	Application
CI/CD Pipelines (e.g., Jenkins, GitLab CI)	Engineers script pipelines using declarative or imperative code to automate security scans. This involves logical sequencing of tasks: if a SAST scan passes, then proceed to build the container; else, fail the build and notify the developer. At a company like Sky, this ensures every software update for their Sky Q platform is automatically vetted for common vulnerabilities before reaching customers.
Infrastructure as Code (IaC) (e.g., Terraform, Ansible)	IaC is used to define secure cloud infrastructure (e.g., on AWS or Microsoft Azure UK datacentres) in configuration files. This relies on set theory and idempotency (a mathematical property meaning an operation can be applied multiple times without changing the

	result) to ensure a server is configured correctly every time it is deployed, eliminating manual errors.
Security Scanning Tools (e.g., Snyk, Qualys)	These tools mathematically analyse code and dependencies for known vulnerability patterns. They produce risk scores (often based on the Common Vulnerability Scoring System - CVSS) which are calculated using formulae that consider factors like exploitability and impact. Engineers interpret these scores to prioritise remediation efforts.
Programming/ Scripting (e.g., Python, Go)	Python is heavily used for writing custom security automation scripts and data analysis. For example, an engineer might write a Python script using the Pandas library to statistically analyse access logs from their London-based datacentre, identifying patterns of suspicious activity that off-the-shelf tools might miss.
Cloud Platforms (e.g., AWS, Azure)	Managing cloud resources involves understanding concepts like cost optimisation through mathematical modelling of usage patterns. Engineers also configure monitoring services like Amazon CloudWatch, setting alarms based on statistical thresholds (e.g., "trigger an alert if CPU utilisation exceeds 95% for 5 minutes").
Threat Modelling Frameworks (e.g., STRIDE, DREAD)	These frameworks provide a structured, quasi-mathematical approach to identifying threats. The DREAD model, for instance, involves scoring threats on a numerical scale for Damage, Reproducibility, Exploitability, Affected users, and Discoverability to calculate a overall risk rating.
SIEM Systems (e.g., Splunk, Elasticsearch)	A Security Information and Event Management (SIEM) system aggregates log data. Engineers write correlation rules using statistical and logical operations to detect complex attack sequences. For example, a rule might be: "Alert if more than 10 failed login attempts occur from 5 different countries targeting a single admin account within a 10-minute window."

Typical Pathway: The pathway typically begins with strong GCSEs (especially in Mathematics and Computer Science) and A-levels in Mathematics and/or Physics. Most professionals hold an undergraduate degree in Computer Science, Cyber Security, or a related STEM field from a UK university; many also pursue postgraduate qualifications. Entry-level positions often include roles like Systems Administrator or Software Developer. Career progression involves moving into a DevOps or Cyber

Security Analyst role before specialising as a DevSecOps Engineer. In the UK, obtaining professional certifications from bodies like (ISC)^2 (e.g., CISSP) or CompTIA (e.g., Security+) is highly valued. For those seeking chartered status, progressing to become a Chartered IT Professional (CITP) through BCS, The Chartered Institute for IT, is a recognised route. Continuous professional development is essential, often supported by UK employers through training budgets.

Industry Demand: The demand for DevSecOps Engineers in the UK is exceptionally high and growing rapidly. The UK government has identified cyber security as a national priority, with a thriving industry contributing billions to the economy. According to the *UK Cyber Security Sectoral Analysis 2023*, the sector continues to see strong growth. Factors driving demand include the accelerated move to cloud computing, stringent data protection laws like UK GDPR, and the increasing sophistication of cyber threats targeting UK businesses. Salaries are consequently very competitive, especially in London and other tech hubs like Manchester and Cambridge.

Real-World Impact: DevSecOps Engineers play a crucial role in protecting the UK's digital economy and critical national infrastructure. Their work ensures that millions of citizens can safely use online banking, government services, and national health services with confidence that their data is secure. For example, the teams implementing secure digital services for HM Revenue and Customs (HMRC) or the NHS COVID-19 app relied heavily on DevSecOps principles. By embedding security into the fabric of digital innovation, these professionals not only protect companies from financial and reputational damage but also help maintain public trust in the technology that underpins modern British society.